DRAFT COPY
PTC NPRM COMMENTS

Supplementary Information

I. Statutory Background

Belknap Freeman

The FRA assumed the posture that it was the source of what is now recognized as Part 236 of Title 49 CFR as it states: "...The FRA has issued regulations, found at 49 CFR part 236" that is technically correct; but it does not address issue, that in the mid sixties, those same rules previously existed under a different part number under the jurisdiction of the Interstate Commerce Commission prior to the existence of the FRA. From a historical standpoint, prior to WW II, the ICC developed the rules from the PRR's CE 223 and documents of other railroads. The entire history of where 236 came from is not stated. FRA leans on these regulations as what's expected when they are in fact a minimum.

II. Regulatory Background

Safetran

The preamble notes "This challenge involves retaining a corporate memory of the intricate logic associated with railway signaling, while daring to use whole new approaches to implement that logic". We agree with the statement and would like to extend it noting that the corporate memory also should include the safety practices and principles used for design, not just the railway logic itself. As computers become more commonplace in our everyday lives, it is easy to become complacent regarding some of the safety hazards they present. As Storey ("Safety-Critical Computer Systems, pg7) points out: "The primary disadvantages of programmable electronic systems in safety-related applications stem directly from their inherent complexity". Yet, we see systems proposed that are highly complex without considering the overall impact of that complexity. I suggest that the FRA sponsor a "white paper" to be written by suppliers who presently have processor-based systems in revenue service identifying what considerations they had in their design and why. This would not be a "How to Design" paper providing proprietary information but would instead be a commentary on what risks have been considered unacceptable and why.

III. RSAC

Booz Allen Hamilton

The FRA should strongly consider continuing the work of the RSAC with regard to this proposed rule and establish a task force to develop a RSPP, PSP, and risk analyses guidelines for an example case.

Belknap Freeman
The introduction of the subject of the Railroad Safety Advisory Committee (RSAC) appears to accomplish several things. Firstly, the composition involves many parties who have no obligation to the railroad in respect to the railroads responsibilities and needs; secondly many on the committees have conflicts of interest, and thirdly they are convenient to relieve the FRA from making any decisions. Even though there might be a railroad representative attending, he can obviously be out voted.

Bob McKnight
The RSAC Committee has quite a few members that have little or no railroad expertise yet are allowed to vote on the development of S&TC regulations, why? FRA forgot to include certain groups that have good experience in railroading (e.g. AREMA, Operation Lifesaver). Have records been kept of the RSAC meetings, especially voting, so one can see who voted and how for a specific item?

IV. Major Issues

A. Why a performance-based approach?

Criteria for evaluation of performance-based approach.

Alstom
It would be helpful if additional guidance and tools were developed to aid in the risk analyses. It would also be helpful if risk numbers and analysis techniques that the FRA finds acceptable, as this rule is applied to real projects, could be made public for use by all suppliers.

Belknap Freeman
The FRA has brought the Aerospace industry into the realm of railroad operation, originally to keep the industry alive in the environment of reduced military purchases. (Thus placing the railroad supply industry in jeopardy). This has been rationalized on the premise that they will bring new ideas; but with this has come a "new culture" of reports and analysis requirements, and those with no idea as to a railroads operation. The results have created a massive increase in parts population and system links. Bringing the airline industry into RR issues is a mistake that will end up adding extra costs, reports, and paperwork by people who do not understand RR operations.
FRA is inconsistent when they state, in respect to risk analysis: "...they provide analysis that suggest the "relative safety" of the projected system in relation to a base case constant against which it is evaluated. But the results do not constitute direct proof that a particular level of safety will be achieved". Now the issue of inconsistency is further evident when the FRA goes on to say: “FRA was not established to regulate risk assessment techniques, and attempting to do so would only inhibit the growth of the discipline..." The above having been stated by the FRA; why do they make risk issues a mandatory reporting issue?

Development of the proposed standard.

Alstom

The statement "demonstrating to a high degree of confidence" (page 42357, Column 1) is subjective. As discussed in numerous RSAC Task Force meetings it is very difficult to define a non-subjective methodology for safety and risk assessment. This is not an exact science. It must be understood that the purpose is to show that the system/product has been comprehensively analyzed for safety. The FRA reviewers of the submittals required by this rule must perform their reviews according to this purpose and not with the desire to meet some arbitrary process, methodology or preconceived documentation format.

Booz Allen Hamilton

The FRA should consider proposing simple criteria for calculation change to baseline risk, thus providing guidance to railroads when performing the risk assessment and avoiding lengthy and costly justifications within each PSP. These proposed standards do not adequately address the complexity and differences associated with the evaluation of different elements of a safety-critical processor based control system. The evaluation of potential risk through the use of deterministic, statistical, and probabilistic analyses and models is strongly affected by many factors and varies from element to element. In order to appropriately manage this effort the Systems designed using engineering judgment may have shown a system is safe but that does not lend itself to quantitative analysis. FRA should consider establishing specific risk assessment guideline or standards for: electrical and electronic hardware; computer, microprocessor, or other programmable devices (i.e. field programmable gate arrays,); software development, verification, and validation; and naturally occurring or induced conditions or environments. These specific guidelines or standards should then be applied to "preferred" decision analysis process that may involve additional risk assessment, modeling, or simulation guidelines or standards.

Advantages of a performance-based standard.

Safetran

Page 42357 column I. "While some of the train control systems may not yield all of the same safety benefits that are supported by traditional track circuits …". This implies that systems based around traditional track circuits cannot provide the core PTC functions, which is incorrect. As an example, the system employed on the Northeast corridor (Cab signal with speed enforcement and ACSES for civil speed, positive stop enforcement) provides all the required functions and is based on conventional systems. Other systems can provide the same benefits. This leaves the question open regarding whether a proposed alternative system can provide equivalent or better safety in a more cost effective manner. Nothing in the rule considers cost effectiveness as part of the evaluation.

Page 42357 Column II. The comments suggest that trains can provide highway grade crossing information “under conditions that are, today, prohibitively expensive”. Analysis has shown that the majority of costs for a highway grade crossing are in areas other than train detection. Unsupported statements such as these tend to confuse the issue and should not be part of the preamble.

Concerns with a performance-based standard.

Alstom

"The lack of complete consensus on the issue of proofs of safety is perhaps best exemplified by the fact that the IEEE standard just referenced does not address validation of these systems". This statement is incorrect. The working group that generated the IEEE 1483 standard purposely decided to concentrate their efforts on the verification activities rather than the validation activities. The group felt that validation activities are well understood and used within the industry but that verification activities were not. The group felt that the development of verification standards would be far more beneficial to the industry. Validation techniques were not 'not addressed' because of a lack of consensus but rather because it was felt that the techniques currently being employed did not need to be standardized.

Page 42359 Column 1: "The FRA fears that the focus will shift to proving that the product is safe enough after it has been designed" Suppliers experienced in this area know that it is not possible to prove something is safe if the product was not designed to be safe from the beginning. In order to reduce the possibility that this rule would cause the focus to change from design for safety to proof it is safe enough can and is handled within the PSP requirements. By requiring the safety philosophy and safety techniques to be defined in the PSP it is necessary for the supplier to identify these techniques and approaches before the design is started.

Page 42359 Column 3: "No amount of research is likely to make risk assessment a pure science…” This is correct. However, the sharing of risk assessment information, methodologies, techniques, etc., will promote understanding and possible consensus on best practices. This is most important in the areas of human factors and existing system risk assessment. Experience has shown that suppliers today, in general, are supplying products and systems that have acceptable levels of risk. It is important that this experience be used and relied on to maintain the level of safety already being achieved.

GE Transportation (Global Signaling)

Page 42358, Column II. Estimates of MTTHE could only be reasonably compared if the derivation methodologies and associated assumptions were identical. Note: If a single methodology is prescribed, whose methodology will be used and who will be forced to re-figure their estimates of MTTHE?

Safetran

Page 42358, Column I. The comments state that suppliers are “not currently able to provide quantitative information concerning the projected life-cycle safety performance of new products” is not correct. Many suppliers commonly provide that type of analysis, particularly for rail transit customers. As part of a voluntary consensus standard (IEEE1483-2000, and IEEE 1473.1-1999), suppliers agreed to provide such a quantitative analysis for rail transit systems. However, it was recognized that the quantitative analysis is only an additional tool to assess the safety of a system. Without a comprehensive qualitative safety analysis to support its assumptions, the quantitative analysis is not sufficient.

Page 42358, Column II. The preamble implies that the development of IEEE 1483 as opposed to a validation standard identifies lack of consensus on proof of safety. This is incorrect. At the outset of the development of that standard, it was recognized that there are many existing standards and Recommended Practices addressing validation that are useful. However, there was no standard addressing the verification of vital functions, so this standard was developed. Further in Column II, it is noted that suppliers were not able to agree on fully quantitative analysis from uniform analytical methods. As noted before, suppliers believe that quantitative analysis without the underlying qualitative safety analyses are misleading and insufficient for judging a system.

Page 42359, Column I. As noted before, we agree with the concern that focusing on quantification refocuses efforts from development to post-design justification. The preamble also notes that software and/or human factors do not lend themselves to quantification, as electro-mechanical systems do. We disagree that electro-mechanical factors lend themselves to quantification. They are analyzed in the same manner as processor-based systems by reducing all implementation aspects of each function, and then analyzing (and mitigating) all possible failure modes for each implementation aspect.

Application to part 235: risk assessments and material modification of systems

Belknap Freeman

The FRA have established, in their proposed rule making, a serious arena where all issues are identified as railroad responsibility, thus setting the stage for all plaintiffs attorneys have a federal basis to claim both "damages" and "punitive damages".

B. How does this proposal affect locomotive electronics and train control?

Alstom

Separating locomotive control and train control functions provides the benefit of allowing the train control functions to be clearly defined and analyzable for safety. Combining these functions will make the safety analysis more complex. If the integration of these functions is allowed, the entire product must be subjected to the requirements for a safety critical product/system.

BRS
It is the opinion of the Brotherhood of Railroad Signalmen that locomotive electronics and train control equipment should be prohibited and remains separate. However, if future technology warrants the integration of locomotive electronics and train control then all facets of the combined equipment must be subject to verification and validation testing under the new performance standards. This should be prohibited and separated from this rule.

Safetran
Because these are inherently non-deterministic, they directly violate basic safety principles described in this section. In addition the user does not have control of the source code of these systems so they can't be comprehensively tested.

(C) What risk assessment methods will be considered adequate?

Alstom
Qualitative risk assessment methods will always be a part of any system risk assessment. It is not possible to determine quantitatively the risk for all areas. All qualitative risk assessments must be accompanied by a reasonable justification.

GE Transportation (Global Signaling)
Both qualitative and quantitative assessments should be allowed to be used depending on the circumstance.

Safetran
A qualitative analysis is essential to a comprehensive analysis. The quantitative portion of the analysis provides a useful tool, but is neither sufficient nor necessary for safety verification. We recognize that this presents an issue for FRA by requiring people skilled in reviewing such a safety analysis. However, this is no less of an issue for quantitative analysis, as there is still the requirement to understand and assess both the underlying qualitative analysis as well as the assumptions used for developing quantitative results. Quantitative analysis is not a +substitute for skilled engineering judgment.

Section-by section analysis

Section 209.11 Request for confidential treatment

BRS
None of the information should be confidential. All information should be readily available in order to ensure the accuracy of any safety analysis.

Belknap Freeman
The subject of proprietary software and obsolescence of software and components is essentially avoided.

GE Transportation (Global Signaling)
It is requested that the FRA confirm that documentation accompanied by requests for confidential treatment in accordance with §209.11(b)-(d) submitted by GET-GS to the FRA to demonstrate compliance with this proposed rule will be accorded confidential treatment. It is also requested that the FRA identify, to the best of its knowledge, any types of submittals under this proposed rule which would not be exempt from mandatory disclosure under 5 U.S.C. §552 (b)(4) of the Freedom of Information Act.

Section 234.275 Processor Based Systems

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236 Application

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236.18 Software management control plan

BRS
The BRS points out that both software and hardware must be subject to the Railroad's Management Control Plan. The interaction of software with hardware directly defines how a component reacts with the system or subsystem. Thus, a Software and Hardware Management Control Plan must be implemented in order to insure that proper software and hardware component revisions for each site and location are documented and maintained through the life cycle of the system and/or subsystem.
Additionally, each railroad should be required to maintain plans at each site and location, along with records of its inventory, which clearly document both software and hardware revisions. Such plans should identify the hardware along with the executive or application software name, software version number, software revision number, date of software revisions, and a description of cyclic redundancy check for verifying PROM contents. The BRS concurs that a 24-month allowance time for compliance is sufficient.

George Dutton
The explanatory material preceding the text of the proposed rule implies that program changes are made only by changing cards in apparatus. However, program changes can be made in a PC (such as is presumably used at a central location) simply through keyboard instructions. How is this method of program change to be controlled and recorded? The explanatory material and proposed rules should provide for this.

GE Transportation (Global Signaling)

Hardware tracking is a necessary element of software management. The supplier should be responsible for supplying initial software configuration information, with the exception of embedded software which is proprietary to the supplier. The supplier should also be responsible for providing the customer with the configurations changes due to modifications and/or upgrades. Subsequently, the railroads should be responsible for tracking and maintaining configurations thereof.

The supplier should be responsible for supplying initial software configuration information, with the exception of embedded software, which is proprietary to the supplier. The supplier should not be responsible for ensuring other products are compatible with the supplier's products. Responsibilities defined within the propose rule between the railroad and the suppliers should be better delineated (see following comments). Suppliers duties should consist of: 1) providing initial software configuration information, with the exception of embedded software which is proprietary to the supplier, and 2) providing software configuration information for changes impacting safety.

A 24-month period may not be sufficient due the significant impact on development processes, documentation requirements, and product development cycle for products already being designed.

Safetran

Configuration management is a potentially difficult area because of the wide variety of potential configurations. Following is one potential method of assigning responsibilities. Suppliers are responsible for maintaining software configuration (version control for released software, as opposed to internal software configuration on source code, etc.) for the Executive Software on individual products and/or systems supplied. (As defined by the FRA, the Executive software is that which remains the same for all applications and is not required to be re-compiled for each application).

In the event that a supplier uses software supplied by others for safety-critical applications, that final supplier (i.e. the one who provides the system to the railroad) is responsible for verifying not only the safety of the externally supplied software, but for maintaining version control for that software. (This last statement does not apply to suppliers who provide applications only on other supplier's equipment (e.g. interlocking controllers). In that case, the original equipment supplier remains responsible for software version control.)

The Supplier software version control shall clearly identify version changes that are necessary for safety as opposed to those that modify functionality. It shall also clearly identify what versions of hardware are required to support the software. If the supplied software supports an interface standard as part of its design, the version control shall also clearly identify the Interface Standard Version (and backwards compatibility if appropriate) that the software is compatible with.

Railroads are responsible for maintaining version control for the Application software used on individual products and/or systems. (They may subcontract this to a supplier if they wish). (The Application software is that which provides external data to the Executive Software causing it to operate as required for a specific application. For example, Application software could be a collection of data describing interlocking operation or car-borne operation. While this data may be compiled through a Configuration File Builder tool, it does not require any re-compilation of the Executive software). Railroads would also be responsible for verifying that all components of a system are compatible with the same version Interface Standard, where appropriate.

Section 236.110 Results of tests

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The results of tests and the changes related to filing and availability of records for inspection fails to indicate any record of any obligation FRA has in insuring their inspector was qualified to know what he was doing. Railroads are getting larger, and an installation can be in one inspector's territory and the records in another inspector's territory -- can he do the job effectively?

Section 236.787a Railroad

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236.901 Purpose and Scope

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236.903 Definitions

MTTHE

BRS
Railroads have indicated objection to the use of the term "average" or "expected" in the definition of MTTHE. The BRS concurs with the language of this definition in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The "Mean Time to Hazardous Event" is troublesome -- if you recognize the potential hazard, fix it. A major issue is not a MTTHE of a component or package; but rather, what is the impact from a complete system?

GE Transportation (Global Signaling)
The use of “expected” or “average” should be allowed in the definition.

Safetran
The term “Mean Time Between Hazardous Events” (MTBHE) is the term in wide use within the rail transit and rail supply industry (reference IEEE 1473.1-1999 and IEEE 1483-2000). Other than creating confusion with existing voluntary consensus-based standards, we have no objection to the MTTHE term. We have no concern with the terms average or expected, as they are part of the term definition. We do recommend that you consider use of the existing IEEE MTBHE definition (“MTBHE: The average time between occurrences of events, where hazardous events and the equipment that may precipitate them are defined at the system level. The hazardous events in the MTBHE are those whose consequences are of a given severity, as determined by the organization generating the safety goals”).

Preliminary Hazard Analysis

Safetran
Typo, It appears this was changed to Preliminary Safety Analysis in rule text.

Validation

BRS
The term “validation” is slightly modified from the IEEE definition to incorporate the notion that validation procedures do not end with the end of the development cycle. Validation can be performed at any stage of a product’s life cycle, including and especially after modifications are made to it. The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

GE Transportation (Global Signaling)
The definition should be left broad to include all stages of a product’s lifecycle.

Safetran
There is nothing inherently wrong with the FRA provided definition of validation. There is a concern that this rule does not make use of existing definitions (e.g. IEEE definitions). Existing definitions and standards were agreed to by in a voluntary, consensus process by Professional Organizations with substantial expertise in the area. Modifying these definitions should only be done with great care.

Section 236.905 Railroad safety program plan

BRS

Section 236.905 Railroad Safety Program Plan (RSPP) Paragraph (c)(2) establishes the timing of the petition process. FRA should respond to the request within 180 days. BRS concurs with FRA's position that the petition is not approved until an affirmative grant from FRA. The BRS recommends an additional 90-day time period for FRA to grant or deny the petition. Paragraph (c)(4) proposes that FRA be able to reopen consideration for any previously approved petition for cause. The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman

One of the nice things concerning a Railroad Safety Program Plan (RSPP) is that it is a new tool for a Plaintiffs Attorney to obtain by "discovery" another document to weave in front of a jury, to represent the railroad as "bad". Why can't the concept of a "safety plan" be incorporated into a revision of one's Safety Rules, Employee's Timetable, or other existing document of instructions? The dialogue related to the RSPP does not indicate that public safety is also a concern.

There is a typo error in the section. 236.915(h) should be referenced as 236.913(h).

Safetran

We agree that the rule creates confusion between risk assessment and safety assessment. Our basic understanding of the process is that a safety assessment must always be done on the underlying products and systems. This safety assessment will be in line with Appendix C and will typically follow existing standards. In addition to the safety assessment, an additional risk assessment will be done on the complete system (including human factors and operational conditions) if there is a substantial change in train control operation, or if the underlying safety assessment is not done in accordance with existing generally accepted practice.

Section 236.907 Product Safety Plan (PSP)

BRS

The BRS concurs with the logic and language contained in paragraph (a)(4) of this section. The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle. The BRS concurs with the logic and language contained in paragraph (a)(12) of this section. The BRS concurs with the language of this section and is opposed to any changes to that language in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman

In discussion of PSPs, the FRA's discussion states in part: "...FRA would require that the applicant compare concepts contained in existing standards to the operational concepts, functionalities and control contemplated for the product...what standards?" They differ on different properties. The rule as written is worrisome, in two respects. First, it does not address the issue of employing "interlocks" to prevent putting devices in the wrong slot, and secondly, if you publish too many warnings, you get into the realm where a good plaintiffs attorney can take the position that a "warning" was not adequate, as compared to other options that might have prevented the hazard. As is typical of the FRA docket, all ultimate responsibility is laid on the railroad, and the task to continue to maintain a life cycle record.

GE Transportation (Global Signaling)

Risk class and safety integrity level are undefined in the Proposed Rule. It appears that this section is referring to the Safety Integrity Level (SIL) classifications found in the referenced CENELEC standards. If so, compliance with non-U.S. standards to meet U.S. regulatory requirements should not be required. Instead, usage of the widely accepted hazard risk index of MIL-STD-810C/D should be specified as being acceptable. The term "formal methods" in software development usually refers to a complicated and time-consuming set of mathematical modeling and formal logic techniques rarely seen outside of NASA and some European systems (Reference NASA Guidebook for Safety Critical Software, NASA-GB-1740.13-96, Section 4.2.3.2). For example, on the SACEM line in Paris, France, formal proofs on 21,000 lines of MODULA-2 code reportedly required 90 man-years of effort. If formal methods of this type are the intent of the referenced paragraph, the level of software analysis required would be overly burdensome to the supplier in relation to the marginal increase in safety achieved. For this reason, it is recommended that the term “methods” be substituted for the term “formal methods”.

The elements in the PSP are adequate and no other requirements need to be included to ensure safety. Also, the level of detail in describing the product is sufficient.

Availability is directly related to safety if fall-back systems/procedures are less safe than the actual system.

Safetran

We would like to emphasize that many of the items listed under the PSP would not be required for many existing processor-based systems. These systems are designed to be independent of railroad operational characteristics as defined under (2) of Section 236.907. Requiring this additional analysis for all systems will substantially increase the cost of their development.

Section 236.909 Minimum performance standard

BRS

The BRS believes it is unnecessary to include language in paragraph (b) that allows the railroads an administrative appeals procedure. In section (e)(3) the BRS concurs with the method of accounting for concurrent changes in operating practices and comments proposing other methods. The BRS also agrees with the conclusion that the failure to make this adjustment would at least theoretically permit a progressive worsening of the safety situation as new technology is brought on line. The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman

"The safety analysis included in the railroads PSP must establish with a high degree of confidence that introduction of the product will not result that exceeds the previous condition". The concept to equate a new product against the "previous condition" questions FRA's judgment in respect to their ordained mission of "safety"; for if a condition had six incidents in a years time, the new product would still pass muster if it was expected to have six incidents in a years time, for then it still will "not result in risks that exceeds the previous condition". If one is making a change, that only needs to obtain the objective that it is acceptable if no better than the one before, why bother?

GE Transportation (Global Signaling)

Train-Miles or Train-Hours would be the most appropriate and useful metric for freight railroads.

US&S

It must be recognized that the proposed Rule adds substantial cost to the procurement of new processor-based signal and train control systems by Railroads. A significant portion of these costs will be incurred in the course of complying with 236.909 (Minimum Performance Standard) along with Appendix B. These require a quantitative risk assessment.

Section 236.911 Exclusions

BRS

The BRS does not agree with the language contained in paragraph (a). The BRS believes that due to the multitude of solid-state equipment in the field that has not had any testing done, these devices should not be "grandfathered" and that they should be subject to the provisions of subpart H. The BRS disagrees with the conclusion that was made by the FRA when they stated: "FRA believes it would be a tremendous burden on the rail industry to apply this subpart to all existing systems, which have to date proven safe."

Particular exception is taken with the concept that the existing systems have to date proven safe. Accidents have happened due to malfunctions of solid-state equipment. Also, FRA is in error to infer that the fact an accident has not occurred is proof of the safety of equipment and/or system. With no testing being done or required there is no proof of safety. As the systems get older and degrade, the industry will experience unsafe conditions and accidents from this degradation, and nothing will be done until after the fact. The BRS believes that the FRA should be proactive and not reactive to this situation and therefore does not support the language as written.
It is critical that FRA enforce the intent of the language in paragraph (c) where the Standards Task Force recommended that a subsystem or component of an office system must comply with subpart H if it performs safety-critical functions within a new or next-generation signal and train control system. - para. (a) Nothing should be grandfathered.

Belknap Freeman
As the FRA appears to be infatuated with the scenario that processor based technology is the ultimate replacement for existing hard wired logic and off the shelf signal equipment they fail to suggest that an installation of processor based technology be compared to the option of installing available of off the shelf equipment and technology (or upgrading an existing installation); which would exceed or be better than that which one has.

Section 236.913 Notification to FRA of PSPs

BRS
The BRS concurs with the language of paragraph (a) as written. The BRS concurs with the language of paragraph (b) as written. The BRS concurs with the language of paragraph (c) as written. The BRS concurs with the language of paragraph (h)(2) as written. The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The FRA discussion, in regard proposed rule 236.913(d) borders on the threat of Federal Blackmail, when it states in part:"... FRA feels it should be involved at the system design review phase of development, thus reducing the scope of FRA review which might otherwise be required. FRA believes that if a railroad does not involve FRA early enough in the process it could potentially delay FRA approval and system implementation, which is often a result of delayed government involvement..."
The proposed rule also completely eliminates and ignores any risk assessment with conventional techniques related to "off the shelf" equipment and methods, either as a replacement or up grade.

It is my opinion that all the various individuals involved in supporting computer models and risk analysis are infatuated with is results that makes the individual feel comfortable; while the truth of the matter is, that one involved has neither the responsibility for or consequences of results. A major flaw of such activity is the lack of ability to actually identify the specific detail of just what hazard exists, such as to allow identification of the problem and lend the opportunity to reach beyond and "fix" the problem.

Bob McKnight

For signal systems only, the railroad owning the tracks in the territory should be required to furnish PSP and RSPP. For train control systems, all railroads operating on the tracks in the territory should furnish joint PSP and RSPP documents. FRA believes railroads should pay for 3rd parties to review documentation. Why only railroads? If FRA does not understand the material presented to it, FRA should pay for 3rd party assistance.

Section 236.915 Implementation and Operation

BRS

The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

GE Transportation (Global Signaling)

Many measures implemented to reduce potential mishap severity in the railroad environment actually lead to a reduction in the likelihood of the worst-case levels of severity. Flexibility in the methodology of risk reduction should be retained in the proposed rules.

Section 236.917 Retention of records

BRS

The BRS concurs with the language of paragraph (a) as written. Records relevant to the current configuration and operation of the system remain available. Period. The BRS believes that FRA should retain the 15-day time period for railroads notifying the FRA of any inconsistency. The FRA should allow the use of e-mail or fax notification.

Belknap Freeman

It would seem that if the FRA followed up with the concept that they suggested, the FRA would participate in design prior to submitting a project for approval, then in addition to the level of documentation required to be submitted in the approval process, they would want the results of tests, and any hazards experienced subsequent to the project being placed into service. It would seem the FRA might care to explore their position of possible liability lawsuits that might arise and would have sufficient basis to pierce the FRA's "Federal Supremacy".

Bob McKnight
In the discussion of record retention for product life cycle no time is specified. However, in Appendix B for Part 236, FRA assumes that a 25-year life cycle will be adequate for products. Although relay based signal & train control systems have a 30-50 year life, processors and computers have a 5-7 year life Some such equipment have been in service longer, but are considered to be technologically obsolete, that is they cannot be replaced in kind. They are no longer manufactured, and replacement units have many features not found in the original equipment.

Section 236.919 Operations and Maintenance Manual

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The discussion of the rule, and the text for the rule, per se, are not in exact agreement; but in any case, certain remarks are impractical. One must recognize, in say a trouble call after hours, say, does not guarantee who or from what direction one might be called; and on an after hours call, the individual could very well have no idea of the nature of the call; thus little information relative to what Maintenance Manuals to bring along. It is suggested that any such maintenance manual should be at "site" in the same manner as one would expect to find an upgraded copy of "circuit plans" for the site in accord with 236. It is to be realized, with a copy at the site, it would minimize the number of copies in existence, along with the background as to where they are at. A significant item when a "revision" exists and there is the necessity to insure all known copies will receive the up date. As to the manual, per se, and proposed rule 236.919(a), should also include the category Test Equipment; such that sub section (a) might read: "..installation, maintenance, repair, modification, inspecting, and testing (and required test gear and tools) of the product and having..." The purpose of such an addition is to insure whatever unique test equipment needed is indicated.
The proposed rule as written, implies, as stated in the discussion, that the plans and manual shall be at the site; but the proposed rule taken literally could authorize having a copy locked up in a drawer at the site, not available to the individual coming "somewhere", to know "where to begin" as out lined in the rule.

Section 236.921 Training and qualification program, general

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The FRA have failed to explore the unexpected consequences such as employees, who in receipt of training, have a new marketable skills resulting in their leaving for other jobs and/or the degraded results of projects they have supported.

Section 236.923 Task analysis and basic requirements

BRS
The BRS concurs with the language of this section in its entirety without revision. Specifically, it is necessary to retain the requirements in paragraph (a)(2) and (a)(3) that the railroad will identify the inspection, testing, maintenance, repairing, dispatching, and operating tasks for the equipment and develop written procedures for performance of same. It is also necessary to retain the language in paragraph (a)(7) that periodic refresher training be conducted at intervals specified in the PSP.

Belknap Freeman
The discussion and proposed rule 236.923, carries an inconsistency, in that either directly or by reference the requirements for listing of qualified personnel would appear to include contractor's personnel. The proposed rule further requires that lists of qualified people be kept. Is the railroad obligated to keep a roster of the contractors personnel when they do not know from what plant or source a contractor's expert might come? The proposed rule 236.923(a)(2) and (a) (3) makes sense; however, it begs to be expanded, such as to precede the Union concept of seniority.

Section 236.925 Training Specific to Control Office Personnel

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236.927 Training Specific to Locomotive Engineers and Other Operating Personnel

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Section 236.929 Training Specific to Roadway Workers

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Appendix B to Part 236 - Risk Assessment Criteria

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The FRA discussion in part (a) of Appendix B Risk Assessment Criterion assumes a twenty-five year service life for various components in a computer-based device. Experience will indicate that many contracts for computer driven devices will not guarantee support for more than 8 to 10 years.

Bob McKnight
Paragraph (h) "FRA imagines that will in most cases perform the actual documenting task." This cost will probably be passed on to the railroads, as is done now. Thus, FRA paperwork requirements will be an additiona1 cost to the railroads.

Appendix C to Part 236 - Safety Assurance Criteria and Processes

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The FRA in Appendix C calls for input from a qualified human factors professional, to be introduced early on in the development stage, and it thus seems to address the supplier, which with reference to a human factors professional just adds to the cost of the product, and could have an impact on possible constraints in a competitive market place. Part (c) goes on to list an extensive list of standards to be used for verification procedures; but the entire Appendix C gets some what vague as to precisely where the matter rests for "Safety Assurance Criterion and Process" -- with the Supplier, the railroad, or both? As listed in the proposed Appendix C (c), there is an extensive list of publications listed, with no supporting information as to their source (or cost) or agency dedicated to produce them. This is particularly questionable as the proposed Appendix specifically states one must have only the latest edition which means there is no way can one expect to go to his local book store and know for certain what the date of it's latest revision is.

Appendix D to Part 236 - Independent review and assessment of V&V

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Belknap Freeman
The third party has no idea of the existing technology that is out there at present; therefore, he can not recognize the inherent risks to safety that exist in the system, as contrasted with other options. This third party will also add unnecessary cost to the system.

Bob McKnight
Concerning the NTSB and its recommendations for Positive Train Separation, since about 1985, three major signal and train control manufacturers have had continuous cab signal and speed control equipment both relay-based and processor-based equipment available. The only major task for processor-based S&TC equipment was developing site-specific application software.

Appendix E to Part 236 - Human Machine Interface (HMI)

BRS
The BRS concurs with the language of this section in order to ensure the safety and integrity of the system throughout its life cycle.

Anticipated Costs and Benefits

Belknap Freeman
The realm of Anticipated Costs and Benefits as seen by the FRA appears to be relegated down to three items as they state in part: "... FRA believes railroads would adopt a new system under their rules only for one or more of the following three reasons:
(1) The new system is safer
(2) The new system is less expensive and will not diminish the existing safety, or
(3) Continued maintenance of the existing system is no longer feasible."
It would seem a prudent man would also add a few more reasons, in making or adopting a new concept to his existing operations, to include:
(a) For the investment involved, what additional benefits accrue?
(b) With increased parts population and added links, many of which are not under the direct control of the railroad, what is the impact of certain consolidated facilities have on the operation of trains?
(c) What additional and anticipated stability of forces would be required?
(d) What level of redundancy for the added links, and the cost and upkeep is required?
(e) What level of support material and test equipment would be required?
(f) What is expected service life and length of guarantee and support would be available?

For starters, the first three reasons offered by the FRA are offered as truths, when in fact they are wrong. One cannot say a system is safer when it does not exist; and has as a crutch, the keeping of a conventional signal system at the bottom to preserve safety.
With only a twenty-five year service life, and the need to date, to keep a signal system in place, plus all the added parts population and additional systems, how can one state that the new concept would be less expensive? If the FRA were to attempt to force their "vision" on the industry, as an unexpected consequence, they could cause the signal supply industry for railroad needs to dry up, thus ultimately cause problems to support present technology. Actually, the FRA's docket goes further to impose delays and uncertainty, as to make a proposed project a gamble as to what to anticipate in coordination with other facilities, such as track, bridges, et al. Such issues of new rules, tests of new facilities prior to being placed in revenue service, all add to uncertainty and coordination problems to an operating facility - time tables, training, et all. The FRA raise the issue, that adopting new technology would be a solution to the issue of no longer being able to maintain existing facilities; however they do not consider a program where one may elect to upgrade their facilities.

GE Transportation (Global Signaling)
The types of risk/safety analyses that suppliers conduct on their products vary based on the type of product, its complexity, new versus proven technology, background of the safety engineers, etc. Revising existing supplier practices to comply with the detailed and restrictive provisions of the Proposed Rule will require much more than simply “gathering of that safety information into one source”. The table on p. 42382 estimates the burden of performing a full risk assessment to be 1000 hours, and developing a PSP to be 80 hours. It is strongly suggested that FRA has underestimated the burden of complying with the Proposed Rule by at least a factor of three. It is recommended that FRA undertake additional cost analyses using input from suppliers, railroads and third party assessor in order to ascertain the true cost of implementing this regulatory action.

Bob McKnight
FRA says the proposed rules will require substantial safety documentation from the railroads. The question of whether costs exceed benefits, . . . "FRA does not believe so. It appears that the costliest part of the documentation will be the risk assessment. Currently, a substantial portion of this work is performed by the suppliers." Several suppliers have told me they now charge the railroads for documentation. If not, the supplier’s costs will increase so they might well increase their product prices. Ultimately, the railroads will pay these documentation costs. Using existing processor-based systems, railroads will maintain a software management plan. Here again, FRA believes benefits will outweigh costs, but can't quantify. "In short, FRA does not know the magnitude of the benefits and costs because of the performance standard concepts embodied in the proposed rule, but believes that benefits will outweigh costs." This last sentence is pure wishful thinking on the part of FRA.

PART 236 (Rule Language)

236.0 Applicability

(f) The requirements of subpart H of this part apply to safety-critical processor-based signal and train control systems, including subsystems and components thereof developed under the terms and conditions of that subpart.
Safety-critical, as applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel and/or equipment, or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist. - §236.903

GE Transportation (Global Signaling)
The proposed rule does not distinguish between vital functions and systems which must be implemented in a fail-safe manner, and non-vital but safety-critical functions and systems which need not be intrinsically safe. As currently worded, the proposed Rule would require a full Railroad Safety Program Plan (RSPP), supplier Product Safety Plan (PSP), risk assessment, etc., as well as FRA approval, for most non-vital control products which contain a processor. Compliance with this requirement would represent a significant cost impact to the rail industry without providing an appreciable increase in system safety. It is recommended that non-vital functions and systems (as determined by a credible Preliminary Hazard Analysis and Functional Fault Tree Analysis) should not be subject to the requirements of subpart H.

LIRR
No exception taken with this section.

PATH
(b)(2) - PATH is a rapid transit operation in an urban area that is not part of the general railroad system of transportation. The revised requirements of Part 236 therefore do not apply to PATH.

236.18 Software management control plan

AAR

Amend the second sentence as follows: The plan must further *describe how the proper software configuration is to be identified and confirmed in the event of replacement, modification, and disarrangement of any part of the system*. It would be impossible to identify in advance all the testing required as a result of replacement, modification, or disarrangement of microprocessor-based systems (or, for that matter, conventional systems). The purpose of the software management control plan is to identify an overall process for ensuring that "the proper and intended software version for each specific site and location is documented (mapped) and maintained."[8] It is not a product-specific plan. It would cost millions of dollars and require large amounts of time to try to ascertain all the possible tests that might be needed in the event of replacement, modification, or disarrangement for any product governed by this section. Consequently, instead of requiring identification of the testing required, FRA should require railroads to identify the process they will use to ensure the proper software configuration is in place.

Alstom

The PSP for each product must provide the details regarding the needs for configuration management, change and retest of safety critical products/systems (236.907 item 13). The railroad software management control plan should identify the documentation and procedures to be followed by the railroad. This plan should include the process to be used to identify and track safety critical devices. The PSP should define the specific requirements for each product including identifying the requirements for changes to both generic or non-site specific software and site specific or application software. The PSP should also include any mitigation strategies or techniques used in the product/system to mitigate risk when changes are made to safety critical components. If the railroad makes changes to safety critical products/systems outside those defined by the supplier within the PSP, the railroad should be required to define (in the RSPP) its procedures and requirements for assuring that safety is not compromised.

GE Transportation Systems

Joint responsibility for maintenance of software is difficult or impossible from a supplier’s perspective unless special agreements and arrangements are made to allow unlimited access to the equipment while in service, and authority to control and manage that equipment. Such arrangements may exist, but these are the exceptions and not the “normal” supplier relationships in place today on most railroads. Since most suppliers have limited control over software configuration management after a product has been delivered to a railroad, it would be inappropriate to regulate a “shared responsibility” for this software if not properly managed after delivery. Overall responsibility by the railroad for compliance is consistent with other FRA standards in effect today, and a change specifically applicable to this rule is unwarranted.

LIRR
This section is accepted.

Northern Indiana Commuter Transportation District
This rule seems to apply to railroads even if they do not employ processor-based equipment. Suggest revising rule to state that software management control plan is only need by railroads using processor-based equipment.

PATH
The rule would place strict liability on the railroads for elements of software configuration control that are outside of the railroad's ability to effectively and reasonably monitor and manage. The manufacturers and suppliers should be held accountable for accurate software configuration and compatibility management. Railroads, in many cases, do not have the expertise or manpower to document and verify that each and every individual component, PROM, hardware, and software code at every location is in accordance with the manufacturer's specified version and revision number. This is properly the responsibility of the supplier.
It is also questionable as to what level of detail of the configuration management plan is actually directly relevant to safety-critical issues. Does changing a piece of peripheral hardware (a printer, monitor, keyboard, mouse, etc.) affect the safety of the system? Would a broad interpretation of the proposed rule require documentation to this extreme?

236.110 Results of tests

(a) Results of tests made in compliance with Secs. 236.102 to 236.109, inclusive; 236.376 to 236.387, inclusive; 236.576; 236.577; 236.586 to 236.589, inclusive; and 236.917(a) must be recorded on preprinted forms provided by the railroad or by electronic means, subject to approval by the FRA Associate Administrator for Safety. These records must show the name of the railroad, place, and date, equipment tested, results of tests, repairs, replacements, adjustments made, and condition in which the apparatus was left. Each record must be:

(1) Signed by the employee making the test, or electronically coded or identified by number of the automated test equipment (where applicable);

(2) Unless otherwise noted, filed in the office of a supervisory official having jurisdiction; and

(3) Available for inspection and replication by FRA.

(c) Results of tests made in compliance with Sec. 236.917(a) must be retained as follows:

(1) Results of tests that pertain to installation or modification must be retained for the life cycle of the equipment tested and may be kept in any office designated by the railroad; and

(2) Results of periodic tests required for maintenance or repair of the equipment tested must be retained until the next record is filed but in no case less than one year.

AAR

Delete the phrase "subject to approval by the FRA Associate Administrator for Safety" in subsection (a) and delete subsection (e). In proposed paragraph 236.923(a)(3), delete "written." FRA's proposal does not facilitate implementation of electronic record keeping and does not fulfill its obligations under the Government Paperwork Elimination Act (GPEA). Proposed section 236.110 requires FRA approval of electronic record-keeping systems for tracking test results. The requirement for special approval of automated tracking systems is inconsistent with the GPEA.

Booz Allen Hamilton

The results of tests performed on a system awarded approval under a performance based standard may be required to be held for the lifetime of the product. Recommend including a statement that the tests and proofs of safety that make up the product safety case be held for the projected life of the product.

George Dutton

(a) - This should be revised to make it clear that FRA can and will obtain and publish data as to each railroad showing the extent of each type of facility (miles of road, miles of main interlockings, track, number of number of locomotive units, etc.) and the failure experience of each, both safe failures and hazardous failures, as has been done in the past and as it is or at least was required by other parts of 49 CFR. The paragraph should also be revised to make it clear that FRA can and will publish the results of tests which have been conducted to confirm the safety of each system. The lack of published results makes the tests conducted by UP and BN in the Pacific Northwest practically useless.

LIRR

The rule change that states “preprinted forms…. subject to approval by the FRA Associate Administrator for Safety” is not currently required. The test forms we currently use are not required to be approved by the FRA. Our test forms are revised continually based on new equipment, technology and feedback from field forces and other railroads. This requirement would delay maintenance and projects by requiring prior approval of test forms. The Railroad will continue to follow the requirement that all forms be available for inspection and replication by the FRA.

Bob McKnight
(c)(1) - Why no number of years here? A 25-year life cycle for products is stated in Appendix B to Part 236 (Rule).

236.787 Railroad

LIRR
Noted, no exception taken.

236.901 Purpose and scope

LIRR
Complying with this clause would require a railroad to have personnel (or consultants) who have intimate knowledge of the design of the new Processor Based systems as they are developed by the manufacturers or system integrators. It is doubtful that this is feasible for smaller railroads. Also, we are not sure that the manufacturer will part with all design data for safety evaluation, despite our assurance to keep the data confidential.
The migration of signal personnel from other industries to railroads may pose a problem in implementation and maintaining security of the information. In addition, this is a departure from the current practice, which may impose undue burden on the railroads.
However when any system is developed for exclusive use of the LIRR, such as CBTC, we would comply with this. The section should be amended as being applicable to only such systems.

PATH
(b) The Port Authority Trans-Hudson Corp. (PATH) is a rapid transit operation in an urban area that is not part of the general railroad system of transportation. The revised requirements of Part 236 therefore do not apply to PATH.

236.903 Definitions

AAR
Add a definition of "train control" to proposed 236.903 as follows: *Train control means the primary system that instructs the train operator or other track occupant on speed or authority limits and/or automatically restricts the train or other vehicle to the speed or authority limit.* This proposal contains myriad requirements for signal and train control systems. While various types of signals are already defined at 49 C.F.R. Part 236, "train control" is not. AAR suggests defining "train control" so that the scope of the regulations is clear. AAR's proposed definition makes it clear that the regulations do not apply to systems that tell an engineer what speed to use for operational purposes such as the saving of fuel (as opposed to the maximum authorized speed for safety).

GE Transportation Systems
It is recommended this section be updated to clearly define what type of locomotive-based "signal and train control systems" are within the scope of the new 49 CFR 236 Subpart H. To help clarify this issue, it is recommended that the definition already presented in the preamble to the rule be added to this section in the final rule. Based on the text already present in the preamble, locomotive "train control systems" could be defined as: "Cab Signals and ATCATS systems are appliances that include a separate antenna for interfacing with the track circuit or inductive devices on the wayside. By utilizing the track circuit or wayside device input, the train control system has the ability to automatically apply penalty brake applications and "knock down" the locomotives tractive effort". By defining "train control systems" in this manner, a clear distinction between other locomotive electronics can be established.

LIRR
No exceptions taken with this section.

Bob McKnight
Include a definition of Application Software. Application Software is that software that is site or application specific.

Preliminary Safety Analysis
Preliminary Safety Analysis means the initial PSP analysis which results in a comprehensive listing of all safety functions that a system, subsystem, or component will perform. The analysis will insure that hazards are controlled when they occur, and that the risks associated with such hazards are either eliminated or mitigated prior to further development. (The initial product safety plan analysis methodology that provides a safety plan which regulates quality assurance, development, testing, implementation, and maintenance of each product.)

Bill Petit
This is a typo, it should this be "Preliminary Hazard Analysis"

Railroad Safety Program Plan
Railroad Safety Program Plan (or RSPP) refers to a formal document which describes a railroad's strategy for addressing safety hazards associated with operation of products under this subpart and its program for execution of such strategy though the use of PSP requirements, as described in Sec. 236.905.

Bob McKnight
This is a typo, though should be through.

Validation
Validation means the process of determining whether a product's design requirements fulfill its intended design objectives during its development and life cycle. The goal of the validation process is to determine ``whether the correct product was built.''

Alstom
The definition should be - Validation means the process of determining whether a product's design requirements fulfill its intended design objectives. The goal of validation is to determine "whether the correct product was built." Comment: (not part of definition) This definition covers any and all areas of the design that have an effect on the ability of the design to meet its objectives.

236.905 Railroad Safety Program Plan (RSPP)

(b) What subject areas must the RSPP address? The railroad's RSPP must address, at a minimum, the following subject areas:
(1) Requirements and concepts. The RSPP must require a description of the preliminary safety analysis, including:
(i) A complete description of methods used to evaluate a system's behavioral characteristics;
(ii) A complete description of risk assessment procedures;
(iii) The system safety precedence followed; and
(iv)The identification of the safety assessment process.
(2) The RSPP must require that a copy of any non-published standards be included with the PSP.

Alstom
(b)(1)(ii) - Should be revised to read, A complete description of risk assessment procedures used to benchmark safety/risk levels.
(b)(1)(iv) - Should be revised to read The identification of the complete safety assessment process used to identify and address all safety concerns at all stages of product development.

Booz Allen Hamilton

(b) - What subject areas must the RSPP address? The railroad's RSPP must address, at a minimum, the following subject areas: (1) Requirements and concepts. The RSPP must require a description of the preliminary safety analysis, including: (ii) A complete description of risk assessment procedures. The text states that an RSPP must address 'A complete description of risk assessment procedures'. Because of the dynamic nature of state of the art risk assessment, it may be more appropriate to have the plan refer to an existing standard for risk assessment, or a more detailed procedure to be carried out on a case-by-case basis. Requiring the plan to include the full description of risk assessment procedures may be unduly burdensome, and may work against the stated objective for use of the latest evaluation techniques. Recommend deleting the requirement to include a complete description of risk assessment procedures from the RSPP, and allow a summary description to be included with reference to a complete description in either a recognized standard or detailed procedure.

GE Transportation (Global Signaling)

(b)(2) - This could be interpreted to include any/all of the supplier’s internal standards and procedures related to design verification and validation. GE Transportation Systems - Global Signaling requests that internal supplier standards and procedures be exempt from this provision.

LIRR

Railroad Safety Program Plan: Railroads generally are not involved in the development of new products. Manufacturers dealing with signal systems and equipment take on this responsibility. Railroad expertise is predominantly in the application of the equipment or system, specifically to meet the conditions of the railroad. The areas listed under (b) of the RSPP are beyond the current expertise residing in many railroads. It is unrealistic to expect the user of the system to define important design criteria relating to the design of the equipment. Such knowledge is exclusive to the manufacturer designing the system.
With current emphasis on cost reduction, it is unrealistic to expect personnel with this expertise be available to railroads such as the LIRR. This should be applicable to the development of a system unique for the individual railroad, e.g. CBTC development on the LIRR. All conventional processor equipment developed by manufacturers for use in multiple railroads must be exempt. If the RSPP has been filed by any of the railroads and approved by the FRA, other railroads using the product should be free to evaluate the application data at the first instance and determine if PSP is to be filed. This will reduce the paperwork and cost to the railroad. In addition, the PSP preparation would entail acquiring most of the data from the manufacturers. Railroads are not staffed to get all the data listed in (b) except item 4 on the Configuration Management Control Plan of this section. If we get the data from the manufacturers merely to submit RSPPs to meet the FRA requirements, over time the true significance may be lost.

Northern Indiana Commuter Transportation District
The rule requires railroads to have expertise typically only found at the product manufacturing level and seldom, if ever, at the product application level. It is unlikely that many railroads would possess or be able to obtain the necessary data for 236.905(b).

PATH
Upon submittal of an RSPP, the rule provides that the FRA may "normally" respond within 180 days to the petition, but that the absence of a response indicates the matter is still pending, for an indefinite period. This is contrary to a usual regulatory process where an application is deemed approved if not acted upon in a regulatory agency within a reasonable time. This means that each project that requires FRA approval must allow for at least a 6-month delay during which no substantive progress can be made. A 6-month or more delay would significantly impact the costs and schedule in such projects and delay the implementation of systems intended to improve the safety and economics of rail operations. Even after approval, the FRA is allowed, based on undefined criteria, to reopen a petition for further review, potentially resulting in further delays to implementation, or a possible interruption of service after a system has been accepted and in place for some period.

236.907 Product Safety Plan (PSP)

(a) What must a PSP contain? The PSP must include the following:
(1) A complete description of the product, including a list of all product components and their physical relationship in the subsystem or system;
(2) A description of the railroad operation or categories of operations on which the product is designed to be used, including train movement density, gross tonnage, passenger train movement density, hazardous materials volume, railroad operating rules, and operating speeds;
(3) An operational concepts document, including a complete description of the product functionality and information flows;
(4) A safety requirements document, including a list with complete descriptions of all functions which the product performs to enhance or preserve safety;
(5) A document describing the manner in which product architecture satisfies safety requirements;
(6) A hazard log consisting of a comprehensive description of all safety relevant hazards to be addressed during the life cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence);
(7) A risk assessment, as prescribed in Sec. 236.909 and Appendix B to this part;
(8) A hazard mitigation analysis, including a complete and comprehensive description of all hazards to be addressed in the system design and development, mitigation techniques used, and system safety precedence followed, as prescribed by the applicable RSPP;

(9) A complete description of the safety assessment and validation and verification processes applied to the product and the results of these processes, describing how subject areas covered in Appendix C to this part are either: addressed directly, addressed using other safety criteria, or not applicable;

(10) A complete description of the safety assurance concepts used in the product design, including an explanation of the design principles and assumptions;

(11) A human factors analysis, including a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the product to enhance or preserve safety, and an analysis in accordance with Appendix E to this part or in accordance with other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable;

(12) A complete description of the specific training necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product;

(13) A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations;

(14) An analysis of the applicability of the requirements of subparts A-G of this part to the product that may no longer apply or are satisfied by the product using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled (see Sec. 234.275 of this chapter and Sec. 236.901(c));

(15) A complete description of the necessary security measures for the product over its life cycle;

(16) A complete description of each warning to be placed in the Operations and Maintenance Manual identified in Sec. 236.919, and of all warning labels required to be placed on equipment as necessary to ensure safety;

(17) A complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated;

(18) A complete description of:

(i) All post-implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety-critical tolerances are not compromised over time, over use, or after maintenance (repair, replacement, adjustment) is performed; and

(ii) Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards (see Sec. 236.917(e)(3));

(19) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and

(20) A complete description of all incremental and predefined changes (see paragraphs (b) and (c) of this section).

AAR

(a)(6) - Requires the maintenance of a hazard log containing a description of all safety hazards addressed by a product, along with a threshold limit for each hazard. AAR does not object to the concept of a hazard log. However, the discussion of the hazards to be addressed by the log in the preamble does not correctly describe what constitutes a hazard.
(a)(9) - While the wording of the proposed regulation is acceptable, the discussion of this requirement in the preamble is cause for concern. The preamble states that "verification and validation for safety are vital parts of the development of products and, in certain cases, should be performed by a third party." FRA should not encourage verification and validation by a third party. As the party most knowledgeable about the product, from a safety perspective it is best if the supplier, not a third party, performs verification and validation.

Alstom

General Comment - This section describes the requirements for documenting how a product's/system's safety is assured. It does not describe a plan. The requirements cannot be completed until the product design is complete and validated.

(a)(1) - The requirement for a list of all product components and their physical relationship is excessive. This level of detail will obscure the purpose of identifying safety critical items. The section should be revised to require a description of all components whose characteristics are relied upon for safety and what those characteristics are. In addition a justification for the reliance on those characteristics should be included. The PSP should reference other documents for detailed circuits, layouts, wiring diagrams, mechanical drawings, etc., but they should not be directly included in the PSP. It is important that the PSP limit its scope to the safety critical items to assure that these items are clearly understood and not lost in volumes of less critical information.
(a)(2) - This item should be revised to allow a justification as to why the product is independent of such characteristics as gross tonnage, speed, etc.
(a)(7) - It should be made clear that products/systems which are designed, verified and validated using accepted methods and techniques, including the constraints listed in Appendix C, and which meet the applicable sections of Part 236 A through G, do not require a risk assessment as outlined in 236.909 and appendix B.
(a)(11) - The inclusion of human factors in the risk assessment of products/system is clearly necessary. However, this is an area that appears to be most difficult to quantify. This is an area where suppliers lack expertise and therefore is an area that will until experience is obtained represent the potential for added cost.

Booz Allen Hamilton

(a)(2) - Recommend including a statement that requires the description of the railroad operation to include any limitations or restrictions imposed on the operation due to the processor based system.

(a)(8) - The requirement for a hazard log and hazard mitigation analysis as separate documents should be reconsidered. Hazard logs typically include the mitigation analysis and recommended mitigation strategy. The advantage of this approach is that the hazard and its' resolution are contained in one document, assuring that the problem and resolution are current and valid. Recommend combining the hazard log and mitigation analysis into a single document.

(a)(15) - The Security requirement should be expanded and clarified to identify the types of security required to be addressed, for example does the NPRM wish to consider: Infrastructure security, Information security, Real time data transfer security.

GE Transportation (Global Signaling)

(a)(2) - This description would vary by customer, location and application, and would force the supplier to generate numerous PSPs (and await numerous approvals) for high-volume products intended for multiple customers. Hazard analyses performed at GE Transportation Systems - Global Signaling already account for mishaps caused by over-speed, high/wide loads, human error, etc., and focus on the “worst case” mishap severity and likelihood per the widely accepted guidelines of MIL-STD-882C/D. Generating the detailed information described in this section would be overly burdensome to the supplier in relation to the marginal increase in safety obtained from such information. Alternatively, if FRA determines that this information is necessary for its review, it should specify its inclusion in the Railroad RSPP rather than the Supplier PSP. 236.907(a)(6) The wording of this section implies that quantitative threshold limits would have to be generated for each potential hazard, thus requiring a full quantitative analysis of the affected system. This conflicts with the Rule Supplementary Information which notes that “[t]he proposed rule would allow both quantitative and qualitative risk assessment methods to be used”. p. 42361, col. 2, para. 3. Additionally, attempting to specify thresholds for hazards which may include intangible parameters such as human error, inadvertent/intentional misuse, dependencies on products from other vendors, etc., is simply an exercise in speculation. This is recognized in other industries by the broad acceptance of the tiered mishap severity and probability categories of MIL-STD-882D (Appendix A). For these reasons, it is recommended that the requirement in this section for maximum threshold limits of each hazard be deleted.

LIRR

Railroad should be exempt if a system has already been approved for use in a Class I railroad or transit agency and has been in use for at least 1 year. This section should not increase railroad burden or incentive will be impeded. Maintaining records does not appear to enhance safety.

Bob McKnight

How a manufacturer makes a product function, as long as it does not interfere with other devices, should be the only concern of the regulations because certain product details are proprietary to the manufacturer.

Northern Indiana Commuter Transportation District

This proposed rule requires expertise not typically held by railroads. Many of the items in the PSP may be highly complex and not readily interpreted by a signal engineer and would lead to inconsistencies in interpretation. Railroads should be exempted from developing a PSP for a product that has been accepted by the FRA for the same application on other US railroads.

PATH

The PSP document is required to include a seemingly endless shopping list of documentation, descriptions and analyses. The PSP must also identify and describe how the proposed system meets or exceeds the existing requirements in Subparts A through F by some alternative means. This requires an unprecedented amount of documentation. This will result in higher costs and essentially reinstitute new bureaucratic requirements after a period when the goal was less paperwork and bureaucracy.

The FRA acknowledges that the existing techniques of quantitative risk assessment are so complex and highly technical that very few understand them. Who will prepare the analyses or review and approve them? The railroads do not have the required expertise, and it is unlikely that the FRA has the capability. Those in academia or the defense and aerospace industries are not familiar with railroad operations or with the standards and practices of rail signal and train control design. The FRA may provide a list of pre-approved 3 rd Party risk assessment consultants, but does not define what criteria or process the FRA will use to select such consultants or what circumstances will warrant a decision by FRA to require the railroad to pay for a 3 rd Party re-assessment of its initial risk assessment.

The FRA seems to assume that railroads and suppliers who pay for and prepare a PSP for a specific product or system will provide access to or copies of their PSP to others that plan to use the same or similar system. This is not likely to happen unless the originator of the PSP can recover the cost of their investment and protect any proprietary information it contains.

US&S

Suppliers such as Union Switch & Signal are more than willing and able to provide processor-based products and systems, which enhance the safety of signaling and train control on our railroads. This can be done in a cost-effective manner for all parties involved by modifying the Product Safety Plan (PSP). Item 7 of the PSP should call for a qualitative risk assessment based on U.S. Military Standard 882.

236.909 Minimum performance standard

(d) What is an abbreviated risk assessment, and when may it be used? An abbreviated risk assessment demonstrates that the resulting MTTHE for the proposed product is greater than the MTTHE for the product or methods performing the same function in the previous condition. This determination must be supported by credible safety analysis sufficient to persuade a reasonable decision-maker that the likelihood of the new product's MTTHE being less than the MTTHE for the system, component, or method performing the same function in the previous condition is very small (remote). An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard if:

(1) No new hazards are introduced as a result of the change;

(2) Severity of each hazard associated with the previous condition does not increase from the previous condition; and

(3) Exposure to such hazards does not change from the previous condition.

(e) How are safety and risk measured for the full risk assessment? Risk assessment techniques, including both qualitative and quantitative methods are recognized as providing credible and useful results for purposes of this section if they apply the following principles:

(2) For the previous condition and for the lifecycle of the product, risk levels must be adjusted for exposure. Exposure must be expressed as total train miles (and, as applicable, total passenger miles) traveled per year. Severity must identify the total cost, including fatalities, injuries, property damage, and other incidental costs, such as potential consequences of hazardous materials involvement, resulting from preventable accidents associated with the function(s) performed by the system. A railroad may, as an alternative, use a risk metric in which severity is measured strictly in terms of fatalities

AAR

(d) - States that the mean time to hazardous event (MTTHE) for a proposed product must be greater than the MTTHE for the product to be replaced. The subsection should state that the "MTTHE for the proposed product is greater than *or equal to* the MTTHE for the product or methods" to be replaced. Otherwise, the subsection will be inconsistent with the performance standard, which is "the product will not result in risk that exceeds the previous condition."

(e)(3) - The last sentence provides that in measuring risk for the risk assessment, the previous condition must be adjusted for assumed implementation of systems necessary to support higher train speeds as specified in 236.0, as well as track and other changes required to support projected increases in train operations. The purpose of this provision is unclear. Obviously, the regulations will not require railroads or their suppliers to assess FRA's track standards. If, however, FRA is saying the analysis must be consistent with the train speeds that will be used, AAR has no objection.

Booz Allen Hamilton

(d) - The three requirements to perform an abbreviated risk assessment will be very difficult to prove. In practice it is expected full risk assessments will be required for most systems. If the use of the abbreviated risk assessment is to be pursued additional guidance as to the level of proof required to achieve FRA acceptance is required.

(e)(2) - The text states “Severity must identify the total cost, including fatalities, injuries, property damage, and other incidental costs…” However the final sentence on the section states “A railroad may, as an alternative, use a risk metric in which severity is measured strictly in terms of fatalities”. The requirements appear to allow only two types of severity metric:
-all inclusive 'must'
-fatality only
Recommend that the required severity metric includes as a minimum fatalities and injuries. Other elements such as system damage would be beneficial but do not necessarily need to be mandated. Recommend that the FRA allow elements to be included in severity, beyond fatalities and injuries, to be decided by the Railroad.

GE Transportation (Global Signaling)

(e)(2) - An assessment by a supplier which assesses the monetary value of hazard mitigation versus the monetary value of human life/injury invites significant liability exposure in the event of a subsequent incident involving such a hazard. The Proposed Rule Supplementary Information states that these two severity assessment alternatives will “avoid metrics which could be misconstrued as trading dollars for lives” (p. 42370, col. 3). However, past assessments of this nature undertaken by, e.g., automotive companies have been used against the supplier in product liability litigation which resulted in huge punitive damage awards. Current hazard analysis standards deemed sufficient in other industries define severity categories in terms of qualitative measures of the worst credible mishap resulting from encountering a specific hazard, i.e., catastrophic, critical, marginal. (MIL-STD-882C/D; Hazard Analysis Guidelines for Transit Projects, DOT-FTA-MA-26-5005-00-01). It is recommended that risk assessment criteria required by this Proposed Rule not include estimations by the supplier of cost, injuries and/or fatalities.

GE Transportation Systems

(e) - This section begins with the following statement: “Risk assessment techniques, including both qualitative and quantitative methods, are recognized as providing credible and useful results...” However, the remainder of this proposed rule, including references to Appendix B, specifically limits the acceptable risk assessment technique to only those that are quantitative in nature. Qualitative risk assessment techniques have been utilized successfully throughout this industry as well as others for many years, and should be recognized in the final rule as an acceptable tool for compliance without specific or special approval required by the FRA. Mandating only the use of quantitative risk assessment techniques would create a significant burden on many suppliers and railroads. A similar requirement which mandates quantitative data as part of the risk assessment also appears in section 236.913(g)(2)(ii), and (iv), and should be removed.

(e)(2) - This section mandates requirements for measuring and adjusting exposure and severity in specific terms dictated by the FRA (e.g. total train miles, cost, injuries, fatalities, property damage, etc.). These parameters and the relative risk indices they represent should not be mandated through regulatory action, but managed locally by the responsible railroad and/or supplier agencies.

LIRR

It is suggested that the FRA only qualify the equipment or system proposed, based on the submission of data from the manufacturer only once, for use on any other railroad. Since application of the equipment is always guided by a manufacturer’s manual, safety of the installation is assured. Compliance of this section by the various railroads for the same equipment or system would result in multiple needs of scarce resources by both the railroad and the FRA. It would also compel the railroad to invest in engineering resources currently not available. With the exception of one or two persons at this railroad, others may not even be familiar with the terms used in this clause. Nor is it needed for the operation of the railroad. In the long run the process will impede the adoption of new technology. Senior Management at railroads are often interested in the timely completion of projects and not in the development of technology.

Northern Indiana Commuter Transportation District

This rule requires a railroad to establish that the introduction of a product will not result in risk that exceeds the previous condition. To make such comparison, it will be necessary for railroads to perform a full risk analysis of not only the proposed product, but also the product being replaced. Such analyses may not, and most likely do not, currently exist and railroads will be forced to perform a risk analysis on a product or system that will soon be retired from service.

Apparently, any new product, even a minor new component added to an existing system, will be subject to this rule irrespective of the cost of the product, irrespective of the safety or economic benefit of the product, and irrespective of the cost and benefit of the safety analysis. This rule may potentially result in discouraging many railroads from seeking even

minor technological improvements to their signal and train control systems. The advancement of safety in the railroad industry will be curtailed as a result.
It is suggested that this rule should define when a product or system ceases to be "new or novel". Once accepted for use by any railroad, such products would then be reclassified as "existing" for all railroads and be subject to the exclusions of 236.911.

PATH

This requires the railroad to prove that safety is not degraded from the existing system. The railroad is burdened "to demonstrate that the safety analysis provides a high degree of confidence". It will apparently be up to the FRA's experts to determine what constitutes a "high degree of confidence", since they have already acknowledged that risk assessment for signal systems is more subjective than scientific. In order to compare the existing and proposed systems, a complete risk and safety analysis must be performed on both. What constitutes the "existing system"? Would any quantitative "safety number" assigned to an existing system be truly comparable to an entirely new system?
The rule does not distinguish between a simple modification to an existing system and a complete replacement of an entire complex system. There is also no direct relationship between the severity of hazard risk and the degree of analysis required. Would the replacement of a single vital relay with a new microprocessor alternative require the same level and depth of risk assessments, documentation, record keeping, and approval process as for an entirely new system?
The rule fails to specify or even reference existing international standards that provide appropriate and widely accepted methods to ensure the safety of new technology systems.

US&S

It must be recognized that the proposed Rule adds substantial cost to the procurement of new processor-based signal and train control systems by Railroads. A significant portion of these costs will be incurred in the course of complying with 236.909 (Minimum Performance Standard) along with Appendix B. These require a quantitative risk assessment of not only the new product/system proposed but also the previous condition. The intent behind the above requirement is good. However, methods of quantitative risk assessment are of questionable accuracy, and the results obtained are very sensitive to the input data, which in the first place are sparse and unsubstantiated. Thus the risk assessment will be of questionable value, and it can also lead to the danger of allowing a new, unproven technology to take ownership for the safety of train movement on a railroad, by simply manipulating the data that go into the risk assessment.

236.911 Exclusions

(a) Does this subpart apply to existing systems? The requirements of this subpart do not apply to products in service as of (the date 60 days after publication of the final rule). Railroads may continue to implement and use these products and components from these existing products

(b) How will transition cases be handled? Products designed in accordance with subparts A through G of this part which are not in service but are developed or are in the developmental stage prior to (date of publication of final rule) may be excluded upon notification to FRA by (60 days after date of publication of final rule) if placed in service by 3 years after date of publication of final rule). Railroads may continue to implement and use these products and components from these existing products. A railroad may at any time elect to have products that are excluded made subject to this subpart by submitting a PSP as prescribed in Sec. 236.913 and otherwise complying with this subpart.

(c) How are office systems handled? The requirements of this subpart do not apply to existing office systems and future deployments of existing office system technology. However, a subsystem or component of an office system must comply with the requirements of this subpart if it performs safety-critical functions within, or affects the safety performance of, a new or next-generation train control system. For purposes of this section, office system means a centralized computer-based train dispatching and/or central safety computer system.

(d) How are modifications to excluded products handled? Changes or modifications to products otherwise excluded from the requirements of this subpart by this section are not excluded from the requirements of this subpart if they result in a degradation of safety or a material increase in safety-critical functionality.

(e) What other rules apply to excluded products? Products excluded by this section from the requirements of this subpart remain subject to subparts A through G of this part as applicable.

Alstom

(a) - This section should be expanded to allow systems/products currently being used in other rail-based transportation, which have been accepted as safe, to be excluded. They would only be excluded if they were to be applied to the railroad to perform the same function as they performed in their current application. For example, some light rail projects, which use track that is part of the 'general railroad system', may use audio frequency track circuits. These track circuits are widely used on rapid transit systems but have not been used on the railroads. There would be no value in subjecting these well-established existing products to the requirements of this subpart.

GE Transportation (Global Signaling)
(c) - This provision would presumably exclude the GE TRANSPORTATION SYSTEMS - GLOBAL SIGNALING Train Management PDS/CADIII office system (currently under development) from Subpart H requirements. However, after PDS/CADIII is introduced into revenue service, this section could be interpreted to require a Subpart H risk assessment of PDS/CADIII in the event of the deployment of a new or next generation train control system within its network. PDS/CADIII is designed as an aid to rail system dispatchers, and is not intended to perform vital functions, nor are other known office systems. Therefore, it is recommended that the second sentence of this paragraph be deleted.
(d) - As specified in this section, changes or modifications to excluded products which increase functionality would be required to comply with subpart H. Full and abbreviated risk assessments as described in 236.909 require evaluation of the risks of the previous condition. "Previous conditions" are defined as "the estimated risk inherent in the portion of the existing method of operation that is relevant to the change under analysis (including the elements of any existing signal or train control system relevant to the review of the product)". This could be interpreted to require a subpart H evaluation of the entire product, which had been specifically excluded from subpart H. It is recommended that this section be amended to specify that, with regard to products previously excluded under 236.911(a)-(c), only additional changes or modifications which provide safety-critical functionality be included in the requirements of this subpart, and that previous conditions need not be evaluated.

GE Transportation Systems
(a) - For clarification purposes, it is recommended that the 2nd sentence in this section be modified to read as follows: "Railroads may continue to implement and use these products and components from these products indefinitely as long as no modifications are made which would exclude these products as specified in section 236.911 (d)".
(d) - This proposed requirement as written will cause the retroactive creation of a hazard analysis and risk assessment on a proven product as specified in Section 236.909(d) and Appendix B(c) of the proposed rule. Because most products in service or in development at the release date of the proposed rule will not have a risk assessment performed in accordance with these proposed rules, nor an established baseline MTTHE, suppliers and railroads will be forced to generate these analyses and MTTHE on products already proven in service. Performance of an "abbreviated risk assessment" to justify any change to products in service at the time of release of the final rule seems excessive and likely to represent a significant cost impact to the rail industry. Retroactive creation of risk assessments in strict compliance to the prescribed methods for equipment already proven in service also seems unwarranted and unlikely to affect the overall safety of this equipment. It is recommended that this section be amended in the final rule to allow assessment of product modifications to be completed in any manner determined acceptable to the railroad, as long as it remains "sufficient to persuade a reasonable decision-maker" that the risk is the same or less than the previous condition.

LIRR

Exclusions: This should include PSP/RSPP requirements when the railroad proposes to see a system approved by FRA on another Class I railroad, subject to the application governed by Manufacturer's Manual/ Application guidelines.

Bob McKnight

It is not clear if a railroad buys processor-based signal & train control equipment that is manufactured before this rule or Subpart H applies, when the only change to the equipment is to make the application software site specific.

Northern Indiana Commuter Transportation District

It is suggested that this rule should define when a product or system ceases to be "new or novel". Once accepted for use by any railroad, such products would then be reclassified as "existing" for all railroads and be subject to the exclusions of 236.911.

It is not clear if exemption in (a) applies to products in service on railroad in question or for products in service on any railroad. It is recommended that exemption apply to products in service on any railroad in U.S. Exemption in (d) is subjective and has no effect because a railroad must still perform a safety analysis to determine if a modification results in a degradation of safety.

Railroads should be exempted from developing a PSP for a product that has been accepted by the FRA for the same application on other US railroads.

PHW

Our second conclusion is that section 236.911 is intended to allow those suppliers who have been successfully applying microprocessors to safety critical railroad applications to continue to do so, without creating a new and substantial burden of analytical proof that would do nothing but confirm what current design practice and actual field service have already demonstrated. It is therefore our presumption that within the context of 236.911d, the FRA would not consider product modifications that were caused by implementation details. Likewise, the addition of producing an output for a function that was already controlled within an existing system would not be considered "a material increase in safety critical functionality". Our presumption is based upon what we interpret as the FRA own principals in creating subpart H to address the continually expanding amount of tests, demonstrations and implementations that without subpart H would require the IRA to handle through exemptions. Our designs and implementations have always been governed by the scope of subparts A through G (and others) and we intend to continue to produce systems that fall within their scope.

236.913 Notification to FRA of PSPs

(a) Under what circumstances must a PSP be prepared? A PSP must be prepared for each product covered by this subpart. A joint PSP must be prepared when:

(1) The territory on which a product covered by this subpart is normally subject to joint operations, or is operated upon by more than one railroad; and

(2) The PSP involves a change in method of operation.

(b) Under what circumstances must a railroad submit a petition for approval for a PSP or PSP amendment, and when may a railroad submit an informational filing? Depending on the nature of the proposed product or change, the railroad shall submit either an informational filing or a petition for approval. Submission of a petition for approval is required for PSPs or PSP amendments concerning installation of new or next-generation train control systems. All other actions that result in the creation of a PSP or PSP amendment require an informational filing and will be handled according to the procedures outlined in paragraph (c) of this section. Applications for discontinuance and material modification of signal and train control systems remain governed by parts 235 and 211 of this chapter; and petitions subject to this section may be consolidated with any relevant application for administrative handling.

(c) What are the procedures for informational filings? The following procedures apply to PSPs and PSP amendments which do not require submission of a petition for approval, but rather require an informational filing:

(1) Not less than 180 days prior to planned use of the product in revenue service as described in the PSP or PSP amendment, the railroad shall submit an informational filing to the Associate Administrator for Safety, FRA, 1120 Vermont Avenue, NW, Mail Stop 25, Washington, DC 20590. The informational filing must provide a summary description of the PSP or PSP amendment, including the intended use of the product, and specify the location where the documentation as described in Sec. 236.917(e)(1) is maintained.

(2) Within 60 days of receipt of the informational filing, FRA:

(i) Acknowledges receipt of the filing;

(ii) Acknowledges receipt of the informational filing and requests further information; or

(iii) Acknowledges receipt of the filing and notifies the railroad, for good cause, that the filing will be considered as a petition for approval as set forth in paragraph (d) of this section, and requests such further information as may be required to initiate action on the petition for approval. Examples of good cause include: The PSP describes a product with unique architectural concepts, the PSP describes a product that uses design or safety assurance concepts considered outside existing accepted practices, and the PSP describes a locomotive-borne product that commingles safety-critical train control processing functions with locomotive operational functions. In addition, good cause would include any instance where the PSP or PSP amendment does not appear to support its safety claim of satisfaction of the performance standard, after FRA has requested further information as provided in paragraph (c)(2)(ii) of this section.

(g) How are PSPs approved?

(2) The Associate Administrator for Safety considers the following applicable factors when evaluating the risk assessment:

(i) The extent to which recognized standards have been utilized in product design and in the relevant safety analysis;

(ii) The availability of quantitative data, including calculations of statistical confidence levels using accepted methods, associated with risk estimates;

(iii) The complexity of the product and the extent to which it will incorporate or deviate from design practices associated with previously established histories of safe operation;

(iv) The degree of rigor and precision associated with the safety analyses, including the comprehensiveness of the [[Page 42390]] qualitative analyses, and the extent to which any quantitative results realistically reflect appropriate sensitivity cases;

(v) The extent to which validation of the product has included experiments and tests to identify uncovered faults in the operation of the product;

(vi) The extent to which identified faults are effectively addressed.

(vii) Whether the risk assessment for the previous condition was conducted using the same methodology as that for operation under the proposed condition; and

(viii) If an independent third party assessment is required or is performed at the election of the supplier or railroad, the extent to which the results of the assessment are favorable.

(h) Under what circumstances may a third party assessment be required, and by whom may it be conducted?

(1) The PSP must be supported by an independent third party assessment of the product when FRA concludes it is necessary based upon consideration of the following factors:

(i) Those factors listed in paragraphs (g)(2)(i) through (g)(2)(vii) of this section;

(ii) The sufficiency of the assessment or audit previously conducted at the election of a supplier or railroad; and

(iii) Whether applicable requirements of subparts A through G of this part are satisfied.

(2) As used in this section, independent third party means a technically competent entity responsible to and compensated by the railroad (or an association on behalf of one or more railroads) that is independent of the supplier of the product. An entity that is owned or controlled by the supplier, that is under common ownership or control with the supplier, or that is otherwise involved in the development of the product is not considered ``independent'' within the meaning of this section. FRA may maintain a roster of recognized technically competent entities as a service to railroads selecting reviewers under this section; however, a railroad is not limited to entities currently listed on any such roster.

(3) The third party assessment must, at a minimum, consist of the activities and result in production of documentation meeting the requirements of Appendix D to this part. However, when requiring an assessment pursuant to this section, FRA specifies any requirements in Appendix D to this part which the agency has determined are not relevant to its concerns and therefore need not be included in the assessment. The railroad shall make the final assessment report available to FRA upon request.

(i) How may a PSP be amended? A railroad may submit an amendment to a PSP at any time in the same manner as the initial PSP. Changes affecting the safety-critical functionality of a product may be made prior to the submission and approval of the PSP amendment as necessary in order to mitigate risk.

AAR

(h)(3)(i) - Amend section as follows: *(i) How may a PSP be amended?* A railroad may submit an amendment to a PSP at any time. Whether a petition for approval or an informational filing is required shall be determined by the criteria of section 236.913, i.e., if the amendment itself concerns installation of a new or next-generation train control system, a petition for approval is required. Changes affecting the safety-critical functionality of a product may be made prior to the submission and approval of the PSP amendment as necessary in order to mitigate risk.

This section provides that a railroad may submit an amendment to a PSP "in the same manner as the initial PSP." AAR understands that FRA's intent was for the same policy that applies to the filing of the initial PSP to apply to amendments. That is, if the amendment by itself would be considered to fall in the category of "new or next-generation train control systems, "a petition for approval would be necessary under section 236.913(b). Otherwise, an informational filing would suffice. Nevertheless, AAR is concerned that proposed paragraph could be interpreted as always requiring a petition for approval if the original PSP required a petition for approval. That would not be justified since the typical PSP amendment should be noncontroversial and FRA possesses the authority under proposed section 236.913(c)(2)(iii) to change informational filings into filings for approval should that prove necessary. AAR's amendment provides the necessary clarification.

Booz Allen Hamilton

(c)(2)(iii) - The program for FRA involvement is weighted towards the end of the safety process. It would be of considerable benefit if a planning or development stage PSP were required to be submitted to the FRA for consideration and approval. This would allow FRA to identify to the railroad any fundamental omissions, errors, etc that would prejudice the full PSP. Although this entails some additional assessment by the FRA it is likely to provide significant benefits at the end of a project, with increased confidence that the safety process and overall development will be acceptable even if some of the more detailed analyses may result in comments.

GE Transportation (Global Signaling)

(d)(2) - Although the 180-day notice under both sections (d)(1) and (d)(2) may be appropriate for large complex systems with long cycle-times, there is no provision for a "fast track" for short cycle-time products, including product modifications. Conversely, it is doubtful that the supplier could provide sufficient information to the FRA under section (d)(1), which would allow FRA to provide a detailed finding of compliance within 60 days of the Notice. The extensive PSP requirements listed under 236.907 include deliverables of information which will only be available when the product is nearly finalized, e.g., post-implementation testing procedures, records of component failures, training and test equipment specifications, etc. It is recommended that FRA include a "conditional approval" provision within both sections (d)(1) and (d)(2) which would allow a product to be implemented when the requirements of subpart H have been substantially complied with, but when non-critical data is still being compiled for final FRA submission.

(g)(2)(vii) - As the methodology of this Proposed Rule will almost certainly differ from that undertaken for previous conditions, this section would automatically weigh against approval of the PSP and promote third party assessments of most new product for many years to come. The methodologies used during a previous assessment should not be relevant to risk assessments conducted in accordance with Subpart H, and it is recommended that this section be deleted from the Proposed Rule.

(h)(1)(i) - As the methodology of this Proposed Rule will almost certainly differ from that undertaken for previous conditions, this section would automatically weigh against approval of the PSP and promote third party assessments of most new product for many years to come. The methodologies used during a previous assessment should not be relevant to risk assessments conducted in accordance with Subpart H, and it is recommended that this section be deleted from the Proposed Rule.

GE Transportation Systems

This proposed requirement indicates that "a joint PSP" must be prepared when a product is operated by more than one railroad. Generally, locomotive-based train control systems are used throughout the country by several different railroads. There is no practical means of reporting where or when this equipment is being used. Generating "a joint PSP" for all possible railroads which may operate this equipment would be impractical from a supplier perspective and unnecessary / burdensome from a railroad viewpoint. Instead of generating a "joint PSP" on a particular product, the FRA should recognize the realities of general interchange service and provide approval for a single, product-specific PSP when appropriate for these types of applications. This approach should also eliminate the need to resubmit a PSP for approval anytime an additional railroad begins operations with a product that has already been approved for use in similar service on another railroad.

(h) - This proposed requirement gives authority to the FRA to mandate an independent third party assessment of a product at cost to the railroad and/or supplier when the FRA concludes this is necessary. Third party assessments represent a significant change to FRA policy and would create a substantial burden on suppliers and railroads impacted by this rule. The potential problems introduced by this proposal are numerous: control of intellectual properties; consistent interpretation of various rules and requirements by multiple auditors; limited effectiveness in the development of new technologies; cost impacts; schedule impacts; etc. It is strongly recommended that requirements for third party assessments be removed from this proposed rule, and allow the PSP approval process to be the mechanism for ensuring compliance.

LIRR

Railroad should be exempt from this if a system has been approved by the FRA for use in any other Class I railroad and is in use on that railroad for more than a year, unless the uniqueness of the application calls for PSP to be filed. When a new system is not currently in use on the railroad, and is proposed, the railroad will merely file an informational document and details of the application where a similar system is in use and any changes made to the specific application of the system. The FRA can inspect and satisfy the needs of this section until conditions are met. There is a need to standardize the risk analysis, at least to start the process. Over time this may be refined. At this time we need some guidance as to what the FRA is expecting. Without specific guidance, railroads will not be able to provide satisfactory documentation. It is suggested that the FRA come up with sample PSP/RSPP etc. on any one of the current systems acceptable to the FRA and included in the Appendix. In regard to third party audit, it would be cost and time effective to do it once for application on all railroads and for systems that are uniformly applied based on the manufacturer's manual or instructions. Once approved for use on one railroad there is no need for third party audits as equipment is identical and the system application is based on the manufacturer's recommended application guidelines.

Bob McKnight

(a)(1) - For signal systems the PSP should be prepared by the owning railroad. For train control systems, the PSP should be prepared by all railroads operating over the territory.
(d) - Is this an implied threat that if the FRA is not involved early on then a railroad's application may not be approved. It is also a concern that FRA or its consultants could unwittingly tell others what they saw at another plant. Such early intrusion could stifle innovation.
(h)(2) - Why should only railroads pay for third party consultants. If FRA does not understand the material it should pay for these consultants.

PATH

The rule proposes involvement by the FRA at the earliest stages of product and system design review. This again is an unprecedented direct involvement of a regulatory agency in the design and development of proprietary systems by suppliers and the application of these systems on affected railroads. While the intent may be to expedite the approval process, the result could interfere with the efficient design and development of a system.

US&S

Independent third party assessments should be limited to radically new architectures or technologies. Processor-based products that use well-established safety architectures such as those listed in IEEE Std 1483 need not be assessed or, at most, be subjected only to independent audits/reviews of PSP documentation generated by the supplier(s).

236.915 Implementation and operation

(a) When may a product be placed or retained in service?

(1) Except as stated in paragraphs (a)(2) and (a)(3) of this section, a railroad may operate in revenue service any product 180 days after filing with FRA the informational filing for that product. The FRA filing date can be found in FRA's acknowledgment letter referred to in Sec. 236.913(c)(2).

(2) Except as stated in paragraph (a)(3) of this section, if FRA approval is required for a product, the railroad shall not operate the product in revenue service until after the Associate Administrator for Safety has approved the petition for approval for that product pursuant to Sec. 236.913.

(3) If after product implementation FRA elects, for cause, to treat the informational filing for the product as a petition for approval, the product may remain in use if otherwise consistent with the applicable law and regulations. FRA may impose special conditions for use of the product during the period of review for cause.

Booz Allen Hamilton

This section does not indicate whether the reporting of failures of equipment using this new technology will be required both in the PSP, and/or the reporting of operational field failures per FRA Form D's.

(a)(2) & (3) - It is recommended that the conditions stated in these sections be strengthened to state: "Products will only be considered for continued in-service operation if the Railroad provides FRA with suitable and sufficient detailed justification of the control measures and mitigations in place to ensure the safety of the public, passengers and staff".

LIRR

No exceptions taken to this section.

236.917 Retention of records

(a) What life cycle and maintenance records must be maintained?

(1) The railroad shall maintain at a designated office on the railroad for the life cycle of the product:

(i) Adequate documentation to demonstrate that the PSP meets the safety requirements of the railroad's RSPP and applicable standards in this subpart, including the risk assessment;

(ii) An Operations and Maintenance Manual, pursuant to Sec. 236.919; and

(iii) Training records pursuant to Sec. 236.923(b).

(2) Results of inspections and tests specified in the PSP must be recorded as prescribed in Sec. 236.110.

(b) What actions must the railroad take in the event of occurrence of a safety-relevant hazard? After the product is placed in service, the railroad shall maintain a database of all safety-relevant hazards as set forth in the PSP and those that had not been previously identified in the PSP. If the frequency of the safety-relevant hazards exceeds the threshold set forth in the PSP (see Sec. 236.907(a)(6)), then the railroad shall:

(1) Report the inconsistency to the FRA Director, Office of Safety Assurance and Compliance, 1120 Vermont Ave., NW, Mail Stop 25, Washington, DC 20590, within 15 days of discovery;

(2) Take prompt countermeasures to reduce the frequency of the safety-relevant hazard(s) below the threshold set forth in the PSP; and

(3) Provide a final report to the FRA Director, Office of Safety Assurance and Compliance, on the results of the analysis and countermeasures taken to reduce the frequency of the safety-relevant hazard(s) below the threshold set forth in the PSP when the problem is resolved.

AAR

This section requires the retention of documents, but in the case of those sections electronic record keeping is not singled out for harsher treatment than paper records. Consequently, AAR suggests deletion of the word "written." Alternatively, FRA could add ", in paper or electronic format," after "written."

LIRR

Retention of Records: Should be applicable to totally new major systems unique to the particular railroad such as CBTC. The records to be maintained for other systems should be left to the individual railroads. This is the case for existing processor-based systems. In the case of false proceeds we file applications with the FRA. Railroads already maintain Configuration Management of Software. Periodical FRA tests are documented and maintained. It is suggested the same be continued.

Bob McKnight
(a)(1) - No time or years of life cycle of product. Should be consistent throughout all rules when referring to Life Cycle. However, if different products have different life cycles they should be so stated in the rules. If too many products, rules should state that manufacturer should determine life cycle time for products, which can then be stated in the Product Safety Plan and the Railroad Safety Program Plan documents.

236.919 Operations and Maintenance Manual

AAR
This section requires the retention of documents, but in the case of those sections electronic record keeping is not singled out for harsher treatment than paper records. Consequently, AAR suggests deletion of the word "written." Alternatively, FRA could add ", in paper or electronic format," after "written."

LIRR
Operation and Maintenance: It is the LIRR's recommendations that the railroad will maintain the applicable Manufacturer's Manual and any relevant application information. It is not practical to prepare and maintain a manual for all the new equipment, unless the system is unique to the railroad such as CBTC. However, the railroad will maintain control over the configuration of software as per procedure established by the railroad.

Bob McKnight
This Rule will require a tremendously large volume of paper. Should consider computer disc that could be inserted in a lap top computer for technician who must have this text as he/she visits locations to inspect, text, etc. on equipment. It will require diligent and close attention to keep this manual up to date. No mention of the cost to create this manual is made.

236.921 Training and qualification program, general

Bob McKnight
There is no discussion of the costs involved, which over time will probably be more than the benefits obtained. Once these people are trained and computer literate these technicians will leave the rail industry for jobs with better pay and working hours.

236.923 Task analysis and basic requirements

AAR

This section requires the retention of documents, but in the case of those sections electronic record keeping is not singled out for harsher treatment than paper records. Consequently, AAR suggests deletion of the word "written." Alternatively, FRA could add ", in paper or electronic format," after "written."

(a)(6) - This section provides that direct supervisors must be given the same training as employees installing, maintaining, repairing, modifying, inspecting, and testing safety-critical elements. AAR is unaware of any, request, need, or precedent for such a requirement. There is no safety justification for requiring a supervisor to have the same training as the employees being supervised. The phrase "and their direct supervisors" should be deleted from this paragraph.

(b) - Amend this section as follows: The railroad shall retain records *showing which of its employees is designated as* qualified under this section. This section requires railroads to "retain records which designate persons who are qualified under this section." Clearly, railroads can only be expected to have records for their own employees. A railroad should not be expected to have records for employees of another railroad or a contractor who may perform functions on that railroad.

LIRR

The section as currently written assumes unlimited budget allocation. The scope and extent of training should be determined by the railroad in consultation with the manufacturer. The training will make extensive use of the manuals and other materials prepared by the vendor at the time of introduction of the system. This may be modified over time based on the railroad's experience. Railroads are not in a position to spend considerable sums of money on the development of materials for training. This should be left to the judgment of the railroads, which have considerable experience in training staff for new technology over years. This procedure has already been proven over years.

PATH

This proposal requires the railroad to be responsible for the proper training of not only its own employees, but of all contractors involved, and presumably even for the original equipment manufacturer and suppliers. This is an impossible task and responsibility for a railroad to assume. It must be the manufacturers', suppliers', consultants', and contractors' responsibility to ensure the proper training of their employees. The railroads do not possess the manpower, means, or expertise to provide any such guarantee.

236.927 Training specific to control office personnel

LIRR
Noted.

236.927 Training specific to locomotive engineers and other operating personnel

LIRR
The railroad will develop it's own locomotive engineer training applicable to the system being installed.

236.929 Training specific to roadway workers

Booz Allen Hamilton
The instruction to roadway workers must take account of abnormal operations (e.g. loss of protection provided by the processor based system). Recommend adding the requirement that the instructions to roadway workers include procedures during abnormal operations.

LIRR
The RR will develop it's own roadway worker training applicable to the system installed.

Appendix B to Part 236 - Risk Assessment Criteria

The safety-critical performance of each product for which risk assessment is required under this part must be assessed in accordance with the following criteria or other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable:

(a) How are risk metrics to be expressed?

The risk metric for the proposed product must describe with a high degree of confidence the accumulated risk of a train system that operates over a life cycle of 25 years or greater. Each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis, and the risk value selected must be demonstrated to have a high degree of confidence.

(c) How is the previous condition computed?

Each subsystem or component of the previous condition must be analyzed with a Mean Time To Hazardous Event (MTTHE) as specified subject to a high degree of confidence.

(e) What other relevant parameters must be determined for the subsystems and components?

The failure modes of each subsystem and/or component must be determined for the integrated hardware/software (where applicable) as a function of the Mean Times To Failure (MTTF) (expressed as failure laws), failure restoration rates, and the integrated hardware/software coverage of all processor-based subsystems and/or components. Train operating and movement rules, along with components that are layered in order to enhance safety-critical behavior, must also be considered. System safety-critical design for verification and validation documentation must support the risk-oriented assessment and validate the methodology used to arrive at the assessment results.

(f) How are processor-based subsystems/components assessed?

(1) An MTTHE value must be calculated for each processor-based subsystem and component, indicating the safety-critical behavior of the integrated hardware/software subsystem and/or component. The human factor impact must be included in the assessment, whenever applicable, to provide an integrated MTTHE value. The MTTHE calculation must consider the permanent and transient hardware failure rates (hardware, design and software coding errors), coverage of the integrated hardware/software (application, executive and input/output driver software) subsystem or component, phased-interval maintenance, and the restoration rates in response to detected failures.

(g) How are non-processor-based subsystems/components assessed?

(1) The safety-critical behavior of all non-processor-based components, which are part of a processor-based system or subsystem, must be quantified with an MTTHE metric. The MTTHE assessment methodology must consider the permanent and transient hardware failure rates, phased interval maintenance and fault coverage of each non-processor-based subsystem or component and the restoration rate.

(2) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The non-processor-based quantification compliance must be demonstrated to have a high degree of confidence.

Booz Allen Hamilton

(a) - The requirement to provide each risk metric with an upper bound, as estimated with a sensitivity analysis together with a high degree of confidence will require risk assessment specialists to perform all analyses thus incurring significant cost for (in some cases) little benefit in terms of safety assurance. Recommend that the rigor of risk assessment required is based on the severity associated with the hazard under assessment.

(g)(1) - The text states 'The safety critical behavior of all non-processor based components, which are part of a processor based system or subsystem must be quantified with an MTTHE metric…'. The requirement appears to require component level FMEA (or suitable alternative) analysis of all non-processor-based components which are part of the processor based system. Given the definition of component (element, device or appliance) the requirements imposes a significant amount of work and cost, even if the risk associated with the non-processor based systems may not justify the depth of analysis. Recommend that the rigor of risk assessment required is based on the severity associated with the hazard under assessment.

GE Transportation (Global Signaling)

(a) - This section implies that quantitative risk data must be generated. However, the Supplementary Information provides that "[t]he proposed rule would allow both quantitative and qualitative risk assessment methods to be used, as well as combinations of the two." p.42361, col. 2, para. 3. (See also comments on qualitative risk assessment in paragraph (4) above). It is recommended that this section be amended to specify that the second sentence thereof only applies when a quantitative risk assessment is undertaken.

(c) - This section would require the supplier of a proposed system to perform a quantitative risk assessment of the existing signal or train control system. Unless the system to be replaced was produced by the same supplier, data necessary to produce such an assessment "to a high degree of confidence" would likely be unavailable. Additionally, as noted above, the proposed rule does not mandate a quantitative analysis. Therefore, it is recommended that §236, Appendix B(c), of the proposed rule be deleted.

(e) - There are currently no widely accepted methods of determining the MTTF for the software portions of a product/system. It is recommended that all references to MTTF as it relates to software be deleted.

(f)(1) - There are currently no widely accepted methods of determining the MTTHE based upon human error rates, software coding errors, or software failures. It is recommended that all references to MTTHE as it relates to human error rates, software coding errors, or software failures be deleted.

Bob McKnight

(h) - The suppliers will pass this cost to the railroads. This is being done now and will continue under the new rules where FRA requires the railroads to furnish documentation.

Appendix C to Part 236 - Safety Assurance Criteria and Processes

(b) What categories of safety elements must be addressed?

The designer shall address each of the following safety considerations when designing and demonstrating the safety of products covered by subpart H of this part. In the event that any of these principles are not followed, the PSP shall state both the reason(s) for departure and the alternative(s) utilized to mitigate or eliminate the hazards associated with the design principle not followed.

(1) Normal operation. The system (including all hardware and software) must demonstrate safe operation with no hardware failures under normal anticipated operating conditions with proper inputs and within the expected range of environmental conditions. All safety-critical functions must be performed properly under these normal conditions. The safety of the product in the normal operating modes must not depend upon the correctness of actions or procedures used by operating personnel. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

(2) Systematic failure. The product must be shown to be free of unsafe systematic failure those conditions which can be attributed to human error that could occur at various stages throughout product development. This includes unsafe errors in the software due to human error in the software specification, design and/or coding phases; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

(3) Random failure.

(i) The product must be shown to operate safely under conditions of random hardware failure. This includes single as well as multiple hardware failures, particularly in instances where one or more failures could occur, remain undetected (latent) and react in combination with a subsequent failure at a later time to cause an unsafe operating situation. In instances involving a latent failure, a subsequent failure is similar to there being a single failure. In the event of a transient failure, the system must restart itself without human intervention. Frequency of attempted restarts must be considered in the hazard analysis required by Sec. 236.907(a)(8).

(ii) There shall be no single point failures in the product that can result in hazards categorized as unacceptable or undesirable. Occurrence of single point failures that can result in hazards must be detected and the product must achieve a known safe state before falsely activating any physical appliance.

(iii) If one non-self-revealing failure combined with a second failure can cause a hazard that is categorized as unacceptable or undesirable, then the second failure must be detected and the product must achieve a known safe state before falsely activating any physical appliance.

AAR

(b)(1) - This paragraph states that the "safety of the product in the normal operating modes must not depend upon the correctness of actions or procedures used by operating personnel." While repeating this statement in the preamble, FRA also acknowledges that the statement sets forth an impossible goal since "safety risks associated with human error cannot be totally eliminated by design, no matter how well-trained and skilled the operators are." The inconsistency must be resolved in favor of acknowledging that the human role, and the potential for human error, cannot be completely eliminated. Consequently, AAR proposes deletion of the third sentence in paragraph (b)(1).

(b)(2) - This paragraph states that the "product must be shown to be free of unsafe systematic failure." This also is an impossible goal -- there cannot be 100 percent certainty. AAR suggests rewording the quoted phrase to provide that "the product must be shown to be free of *foreseeable* unsafe systematic failure."

(b)(3)(i) - The penultimate sentence states that in "the event of a transient failure, the system must restart itself without human intervention. " This might not always be possible. AAR suggests rewording the sentence to provide that in "the event of a transient failure, the system should be designed, to the extent feasible, to restart itself without human intervention."

(b)(3)(ii) - Amend the proposed paragraph follows: There shall be no *known* single point failures in the product that can result in hazards categorized as unacceptable or undesirable. Occurrence of single point failures that can result in hazards must be detected and the product must achieve a known safe state before falsely activating any physical appliance. AAR has two concerns with this paragraph as proposed. First, the paragraph seems to be internally inconsistent. On the one hand, the paragraph states that there cannot be any single point failures that can result in hazards. On the other hand, the paragraph states that the occurrence of single point failures that can result in hazards must be detected by the product. The second problem is that the paragraph states the obligation in absolute terms. That is, the occurrence of a failure would be a violation regardless of fault. AAR's proposal resolves these concerns. AAR's proposed amendment makes it clear that railroads are required to address known single point failures.

Booz Allen Hamilton

(b)(1) - The requirements that there shall be no hazards categorized as unacceptable or undesirable is in itself a very stringent performance requirement. However the guidance does not indicate how that measure will be defined. This requirement imposes additional restrictions above the 'no worse than' general risk requirement. Additionally the last sentence 'hazards categorized as unacceptable must be eliminated by design.' Requires that all hazards initially categorized as unacceptable must be eliminated. While this is clearly a good target in practice there will be many hazards that cannot be eliminated but can be reduced to 'acceptable' levels through many mitigation methods including design action. Recommend that the requirements for hazard mitigation be revised to include the commonly used list of preferences (e.g. eliminate, reduce, mitigation, warning, procedure).

(b)(2) - The requirement that the product will be shown to be free from unsafe systematic failures is not achievable. Processes can be employed to reduce the likelihood of systematic failure but they cannot demonstrate 'free from'. The use of the European Standards referenced in the NPRM includes the idea of safety integrity levels. A similar concept should be considered, which aims to minimize the probability of systematic failures through process, while recognizing it is impossible to completely remove them, particularly in complex software systems.

GE Transportation (Global Signaling)

(b)(1) - Many processor-based locomotives controls are not intended to perform vital functions, and thus rely to some degree on the operator to detect failure of such controls and take appropriate actions. This section implies that all processor-based locomotive controls must be designed for vital, fail-safe operation, which would be unduly burdensome to suppliers and railroads without providing an appreciable increase in system safety. It is recommended that this section be amended to read “The safety of the product performing vital functions in the normal operating modes must not depend solely upon the correctness of actions or procedures used by operating personnel.”

(b)(2) - There are currently no widely accepted methods of proving error-free coding outside of conventional best practices in software development, analysis, review, test and process control. Verification and validation can determine if a product meets specifications, but providing demonstrable evidence that specifications are complete and error-free is beyond current industry capability. Further, proving the absence of installation and maintenance errors is even more impractical. As an example, the long-accepted “vital relay” can still fail unsafely if inadvertently installed with the relay permanently energized, or installed upside down such that gravity does not open the contacts under another failure scenario. It is recommended that this statement be deleted from the proposed rule, or amended to require evidence of conventional best practices in software development, analysis, review, test, process control, installation and maintenance.

(b)(3) - Depending upon the source/cause of the transient failure, automatic restart can result in an unsafe state. Instead, the safest state may actually be non-operation until manually initiated by the operator. It is recommended that this section be identified as a guideline rather than a mandate.

Appendix D to Part 236 - Independent Review of Verification and Validation

Alstom

What criteria will be used to determine if the reviewer is qualified to perform as a third party assessor? How will companies, consultants, etc. be qualified to perform this function? Experience has shown that suppliers have had to apply significant resources to the education of the 'third party reviewer'. This is especially true when the third party reviewer's expertise is in safety, but in another industry.

Bob McKnight

Third party or reviewer is a cost to any or all suppliers, railroads or FRA. FRA should consider paying third party reviewers if it needs help. Otherwise it is an additional cost of regulation to the railroads. This will increase the cost side of the benefit/cost ratio.

US&S

The other significant contributor to the increased cost is the requirement for independent third party assessment of the new product. From our experience with such assessments to the European CENELEC Standards, this rest can far exceed the total development and internal verification & validation cost, without yielding any appreciable benefit.
In general, a better approach would be to rely heavily upon the experience and expertise of suppliers who have been involved in designing and furnishing safety-critical processor-based systems over the last two decades. The process and discipline that go into the development, verification and validation of these products are more important and add more value than probabilistic risk assessments and third party certifications.

Appendix E to Part 236 - Human Machine Interface (HMI) Design

(c) What kinds of human factors issues must designers consider with regard to the general function of a system?

(1) Reduced situation awareness and over-reliance. HMI design must give an operator active functions to perform, feedback on the results of the operator's actions, and information on the automatic functions of the system as well as its performance. The operator must be ``in-the-loop.'' Designers shall consider at minimum the following methods of maintaining an active role for human operators:

(i) The system must require an operator to initiate action to operate the train and require an operator to remain ``in-the-loop'' for at least 30 minutes at a time;

(ii) The system must provide timely feedback to an operator regarding the system's automated actions, the reasons for such actions, and the effects of the operator's manual actions on the system;

(iii) The system must warn operators in advance when they require an operator to take action; and

(iv) HMI design must equalize an operator's workload.

(d) What kinds of HMI design elements must a designer incorporate in the development of on-board train displays and controls?

(1) Location of displays and controls. Designers shall:

(i) Locate displays as close as possible to the controls that affect them;

(ii) Locate displays and controls based on an operator's position;

(iii) Arrange controls to minimize the need for the operator to change position;

(iv) Arrange controls according to their expected order of use;

(v) Group similar controls together;

(vi) Design for high stimulus-response compatibility (geometric and conceptual);

(vii) Design safety-critical controls to require more than one positive action to activate (e.g., auto stick shift requires two movements to go into reverse); and

(viii) Design controls to allow easy recovery from error.

GE Transportation (Global Signaling)

(c)(1)(ii) - Blanket application of this section to all HMIs could result in information overload to the operator, or delays in critical information due to feedback of irrelevant information such as “the reasons for such actions”. It is recommended that this section be identified as a guideline rather than a mandate.

(d)(1)(vii) - Blanket application of this section to all HMIs could result in delays in operator actuation of controls in emergency situations, or frustration of operators required to perform multiple actions to operate common controls which could be considered safety-critical. It is recommended that this section be identified as a guideline rather than a mandate.

General Comments

AAR

AAR believes the table setting forth the estimated costs of the proposed information collection requirements significantly understates those costs. AAR would be pleased to provide further information as FRA proceeds to complete its analysis of the costs of these regulations.

The second full paragraph on p. 42368 of the preamble is unclear. There is no apparent relationship between the first two sentences and the rest of the paragraph. Consequently, AAR cannot discern the import of the last part of the paragraph.

The performance-based approach embodied in the NPRM represents a significant step forward in FRA's approach to regulating the railroad industry. AAR strongly supports FRA's decision to adopt innovative performance standards.

Alstom

The preamble to the proposed rule contains significant information about the interpretation and purpose of the rule. This preamble information should be included in the rule as an appendix to aid in consistent understanding and interpretation of the rule.

The need to define the risk of an existing system and the effects of adding a new system seems reasonable, conceptually. However, as evidenced by the attempts of UVA to develop a tool, the practicality of actually completing this task is questionable. The results of the UVA efforts to date are certainly not conclusive nor has there been a consensus agreement on their correctness. It is necessary that the rule allow sufficient flexibility in this area to allow the rule's intent to be achieved. The intent is to show that the new system does not adversely affect the safety of the railroad. It may be necessary to complete this proof in a more subjective manner than is proposed by the UVA process.

GE Transportation (Global Signaling)

Given the clear need to balance the requirements to create an environment to prove new and novel train control systems with the need to preserve the present methodologies without imposing unnecessary and unproductive analyses, as well as the need to provide equitable solutions to the rail industry's constituents, the following general recommendations are respectfully submitted for serious consideration.

1. Explicitly exempt all future train control products / systems (or modifications to existing products / systems) from the requirements of Subpart H if it can be demonstrated through a simple Preliminary Hazard Analysis (PHA) that such new products / systems are constructed using established / proven principles, techniques and/or methods substantially similar to those used to implement existing products / systems that are already exempt from the requirements of Subpart H.

2. Explicitly exempt all locomotive on-board products / systems from the requirements of Subpart H except for those directly involved in the signaling and train control functions**.**
3. Prior to implementation, conduct a study to demonstrate that the implementation of this rulemaking is consistent with FRA's own criteria for promulgation… specifically… Simplicity, Relevancy, Reliability, Cost & Objectivity.
4. Revise the rule to allow Product Safety Plans (PSPs) to be developed such that they have plenary applicability over many territories.
5. Eliminate the need for the development of a base line safety analysis when the intended upgrade utilizes vital products and the associated safety upgrade is self-evident.
6. Consider the establishment of a minimum goal for "Mean Time to Hazardous Event" (MTTHE) when the anticipated baseline change removes human oversight from the prevailing control methods. Such minimum goals could be established for each of the three core PTC functions (Positive Train Separation, Enforcement, & Protection of Roadway Workers and Equipment).

GE Transportation Systems

The preamble section of the proposed rule includes time and cost estimates which have been generated by the FRA to reflect approximate impacts to the industry to comply with all provisions of the proposed rule. GETS feels these estimates are significantly underestimated and would suggest that an increase by a factor of ten (10) may be more appropriate for many of the tasks listed. A significant amount of time and money will have to be spent to justify why a trivial modification to an existing product does not represent cause for a "full risk assessment". The costs associated with the purely administrative processes, informational petitions and filings, test result forms, records retention, etc., will also add a significant time and cost to the current process. All of these costs will be passed imposing economic impacts across the industry that are not accurately reflected in the proposed rule. It is strongly recommended that a more comprehensive evaluation of estimated costs introduced by this proposed rule be completed prior to formal regulatory action.

Given the potential implications of these new rules and their possible effect to broad range of entities who contribute to the North American Rail Industry, GETS recommends that a public hearing(s) be arranged to facilitate further dialog on this subject and help ensure all appropriate facts and opinions are being considered in this rulemaking process.

Bob McKnight

The FRA should withdraw the proposed rules in docket 2001-10160 for reconsideration and revision for the following reasons:

- The proposed Rule will involve revisions to 6 existing rules in 49 CFR Parts 209, 234 and 236. Additionally, a new Subpart H of Part 236 adds 15 new rules as well as 4 Appendices B-E to Part 236.
- - There will be additional paperwork requirements and associated costs to meet 12 document-reporting requirements. The 12 reports, letters, records or documents that a
- railroad must submit to FRA (see FR August 10, 2001, Page 42382) would require 638 responses, mark 10,000 components and keep 4,400 records. The total cost to a railroad would be $2,130,539. Omitted from the discussion is any indication of the length of these reports. Are they 1 pager 10 pages or what? The fact that there are no examples of any of these reports, their size is apparently not able to be defined by FRA. In effect, this is an unfunded mandate by FRA to the railroads: "Send us all the information you can on a new processor-based system and we will decide if it is enough or correct."

- These proposed rule changes and new Subpart H are definitely going to be a paperwork and cost burden to the railroad companies. These costs could be particularly onerous to short line railroads.

- These proposed rules could well retard innovation. Rather than go through the paperwork burden and its cost, a railroad might well install relay based signal and train control systems.

- Present processor-based S&TC systems have good safety records.

Northern Indiana Commuter Transportation District

Proposed Rule 236 Subpart H as a whole is certain to stifle technological advancement in the signal and train control industry and hence ultimately suppress the enhancement of rail safety.

PATH

In its Supplementary Information, Section IV, Major Issues, FRA notes that the proposed standard “would require extensive documentation of the safety of the system prior to its introduction in revenue service.” The requirements within the proposed rule represent an unprecedented level of documentation, analysis, and FRA approval involvement. This will place an excessive, unfunded burden on some railroads that could offset to a substantial amount any economic benefit that might result from the use of the new technology.

The manufacturers and suppliers of these systems have acknowledged in their comments that the proposed rule will significantly increase the costs of those systems. This is not consistent with Federal efforts. The proposed rule requires quantitative risk assessments not only of any planned new processor-based signal system, but also of existing systems. The costly assessments and analyses required would therefore be subjective and generally inconsistent across the varying submittals from the many different railroad organizations required to comply with this rule. This seems also to imply that there could be an ever-changing level of expectations and requirements to meet for approval.

The subjective "art" of risk assessment is required to be sufficiently convincing to "persuade" FRA to approve a particular petition. Such open-ended generalities provide no guidance or assurance for the railroad on the likelihood of an approval after investing an excessive amount of often-public resources in time, manpower, and cost. This rule is therefore more likely to discourage railroads from pursuing new, potentially more economic, technology due to the uncertainty and excessive burdens placed on such systems by the proposed rule.

In the discussion on Regulatory Impact, the FRA claims this rule will facilitate new technology "under minimal government scrutiny" yet the rule itself expands the FRA's involvement and approval jurisdiction from the earliest stages of a product or system's design and development, throughout the system's expected life cycle. The rule imposes a high cost penalty on the use of new technology by requiring extensive, detailed analyses, record keeping, and lengthy delays in approval processes and implementation.

The FRA admits that it "does not know the magnitude of the benefits and costs" of its proposed rule yet it would impose this unquantified burden on railroads already burdened with bureaucratic oversight. Considering the detail and depth of the analyses required by the rule, it is believed that the time and cost estimates provided by the FRA are significantly understated.

US&S

Processor-based s&tc equipment has not contributed to an accident in the USA or elsewhere. Factors such as human error, poor maintenance, unsafe practices, etc. have been the main causes behind RR accidents. Public interest can be best served if FRA and the nation's RRs focus their attention on these factors and take a more pragmatic approach to technology advances in s&tc systems.

It is unclear if the FRA has the authority to regulate the manufacture, distribution, and sale of any type of s&tc equipment under 49 USC 20103 or 49 USC 20502.

It is unclear if the FRA has or will have the budget and manpower to carry out the technical and administrative tasks described in the proposed rule.

With reference to specific issues such as broken rail detection and the future of continuous inductive cab signaling, we urge the FRA to hold the line and continue to uphold the technical requirements that have successfully withstood the test of time.